THEORY OF NUMBERS

PART I.

Cambridge:
PRINTED BY C. J. CLAY, M.A. AND SONS,
AT THE UNIVERSITY PRESS.

THEORY OF NUMBERS

PART I.

BY

G. B. MATHEWS, M.A.

FELLOW OF ST JOHN'S COLLEGE, CAMBRIDGE;
PROFESSOR OF MATHEMATICS IN THE UNIVERSITY COLLEGE OF NORTH WALES.

CAMBRIDGE:
DEIGHTON, BELL AND CO.
LONDON: GEORGE BELL AND SONS.
1892

PREFACE.

THIS treatise is intended to provide the English student with an intelligible outline of the Theory of Numbers which may serve as an introduction to the detailed study of the subject at first hand. No single work of reasonable size could possibly do justice to every part of the theory; and in the choice of material it is not easy to adopt any plan which is likely to approve itself to everyone. I have been guided principally by a desire to give a fairly complete account of the theories of congruences and of arithmetical forms, so far as they have been developed hitherto; to this I hope to be able to add a sketch of the different complex and ideal theories. Diophantine analysis proper, and questions of pure "tactic," have been omitted, except in so far as they have been subsidiary to the general scheme.

The range of this first volume is sufficiently indicated by the table of contents. It is hardly necessary to say that I have derived continual assistance from the works of Gauss and Dirichlet, and from H. J. S. Smith's invaluable *Report on the Theory of Numbers.* I am also greatly indebted to Professor Dedekind for permission to make free use of his edition of Dirichlet's *Vorlesungen über Zahlentheorie.* So far as this present volume is concerned, the account of Dirichlet's researches has been taken primarily from his original memoirs; at the same time, I owe much to the study of the *Vorlesungen,* and I hope that I may eventually avail myself of Prof. Dedekind's kindness more directly, by giving some account of his theory of ideals.

In the references at the ends of the chapters and elsewhere I have done my best to indicate fully the sources from which I have derived my information. No attempt has been made to give an exhaustive bibliography; even if I had been equal to the task of compiling it, the result would probably be merely embarrassing to the beginner, whose attention should be directed in the first place to the works of the great masters of the science.

Several friends, among whom I may mention Mr H. F. Baker, of St John's College, Cambridge, Mr R. W. Hogg, of Christ's Hospital, and Mr A. G. Greenhill, have kindly allowed me to send them proof-sheets; Mr J. Hammond has been good enough to revise my account of Professor Sylvester's researches on the distribution of primes; and I am indebted to my colleague, Mr A. Gray, for advice and assistance in seeing the book through the press. To all of these my best thanks are due; and I may add that I shall be grateful for any criticisms or corrections that may be sent to me by any of my readers.

G. B. MATHEWS.

University College of N. Wales,
Bangor.

CONTENTS.

CHAPTER I.

DIVISIBILITY OF NUMBERS. ELEMENTARY THEORY OF CONGRUENCES.

CHAPTER II.

QUADRATIC CONGRUENCES.

CHAPTER III.

BINARY QUADRATIC FORMS; ANALYTICAL THEORY.

CHAPTER IV.

BINARY QUADRATIC FORMS; GEOMETRICAL THEORY.

CHAPTER V.

GENERIC CHARACTERS OF BINARY QUADRATICS.

CHAPTER VI.

COMPOSITION OF FORMS.

CHAPTER VII.

CYCLOTOMY.

CHAPTER VIII.

DETERMINATION OF THE NUMBER OF PROPERLY PRIMITIVE CLASSES FOR A GIVEN DETERMINANT.

CHAPTER IX.

APPLICATIONS OF THE THEORY OF QUADRATIC FORMS.

CHAPTER X.

THE DISTRIBUTION OF PRIMES.

CORRIGENDA.

Page 31. The account of factor-tables requires amendment. Burckhardt's tables extend from 1 to 3,036,000; those of Dase, continued by Rosenberg, comprise the seventh, eighth, and ninth millions; and the tables for the fourth, fifth, and sixth millions have been published by J. Glaisher.

Page 145, line 17, *for* q_2 *read* q_0.

Page 200, line 7, *for* $x \equiv -6, 12, 14$ *read* $x \equiv -4, -6, -11$.

Page 255, last line, *for* $2\Pi(1 - r^b)$ *read* $4\Pi(1 - r^b)$.

CHAPTER I.

Divisibility of Numbers. Elementary Theory of Congruences.

1. THE whole of arithmetic is based upon the conception of whole numbers, or integers, and upon the application to them of the four fundamental processes of addition, subtraction, multiplication, and division. The direct operations of addition and multiplication obey the laws of commutation, association, and distribution, which are expressed by the formulae

$$a + b = b + a$$

$$a + (b + c) = (a + b) + c$$

$$ab = ba$$

$$a \, . \, bc = ab \, . \, c$$

$$a(b + c) = ab + ac$$

all of which may be verified intuitively, as soon as the conceptions of adding and multiplying whole numbers have been correctly acquired.

The inverse process of subtraction leads to the enlargement of the domain of arithmetic by the introduction of the idea of negative integers, and the establishing of the "rules of sign." Finally, the idea of division is generalized so as to give rise to the theory of rational fractions, positive and negative.

Strictly speaking, the theory of numbers has nothing to do with negative, or fractional, or irrational quantities, *as such*. No theorem which cannot be expressed without reference to these notions is properly arithmetical: and no proof of an arithmetical theorem, or solution of an arithmetical problem, can be considered finally satisfactory if it intrinsically depends upon extraneous analytical theories. At the same time a great deal is gained in simplicity and clearness of statement by the admission of negative integers, and the application of the algebraical rules of sign: so that in future the term "integer" or "whole number" or simply "number" (where there is no risk of ambiguity) will be used as equivalent to "positive or negative whole number."

2. A number a is said to be divisible by another number b when a third number q can be found such that $a = qb$: a is also said to be a multiple of b, and q is called the quotient of a by b; finally, b is said to be a divisor of a.

If a is divisible by b, it is also divisible by $-b$. Namely $qb = (-q)(-b)$: so that if $a \div b = q$, $a \div (-b) = -q$. The divisors b, $-b$, are not considered to be distinct.

Every number a, which is different from $+1$ or -1, has at least two distinct divisors, namely 1 and a. If it has no divisors distinct from them it is called a prime number, or simply a prime: if otherwise, it is said to be composite.

Two numbers are said to be prime to each other, or relative primes, when they have no common divisor except $+1$ or -1. For example, $(20, 21)$, $(-15, 49)$.

The product of two positive integers, each less than a given prime number p, cannot be divisible by p.

For let a be positive and less than p, and suppose, if possible, that ab, ac, ad, etc. are divisible by p, where b, c, d, etc. are all positive and less than p. There is only a finite number of integers which are positive and less than p: hence one of the numbers $b, c, d\ldots$ must be less than any of the rest: let this be b. Evidently $b > 1$: otherwise a would be a multiple of p, and at the same time less than p. Now p being prime is not divisible by b: hence we may write $p = mb + b'$ where m, b' are positive integers and $b' < b$. Since ab is a multiple of p so also is mab. Put $mab = \lambda p$, so that λ is a positive integer. Then

$$\lambda p = mab = a \,.\, mb = a(p - b')$$

whence

$$ab' = (a - \lambda)p:$$

that is, ab' is a multiple of p. But $b' < b$: so that this contradicts the hypothesis, according to which b is the *least* positive integer such that ab is a multiple of p. The proposition is therefore true.

Corollary 1. If a, b are any numbers not divisible by p, their product is not divisible by p.

For we may always put $a = \lambda p + \alpha$, $b = \mu p + \beta$, where λ, μ are integers, and α, β are integers positive and less than p. Hence

$$ab = (\lambda\mu p + \lambda\beta + \mu\alpha) p + \alpha\beta :$$

and if ab were divisible by p so also would be $\alpha\beta$, contrary to the proposition just proved.

Corollary 2. If $a, b, c, d\ldots$ are all prime to p, their product is prime to p.

This is proved by repeated application of Cor. 1.

3. Every composite number can be resolved into prime factors, and this can be done in only one way.

Let A be a positive composite number. Then since it is composite, it has at least one positive divisor m which is greater than 1 and less than A. Suppose then that $A = mm'$. If m and m' are both primes, the resolution has already been effected: if not, the process may be repeated, viz. either m or m' or both may be resolved into two factors, and so on. It is clear that eventually no further resolution will be possible, because if A could be resolved into the product of an infinite number of integral factors, each greater than 1, it would be infinitely great. Now applying the commutative law of multiplication, A is finally reduced to the form

$$a^\alpha b^\beta c^\gamma \ldots$$

where $a, b, c \ldots$ are different positive primes.

It is clear that if two resolutions are possible the same prime factors must occur in both; otherwise Cor. 2 of last article would be contradicted: so that the only admissible supposition is

$$A = a^\alpha b^\beta c^\gamma \ldots = a^{\alpha'} b^{\beta'} c^{\gamma'} \ldots$$

where $a, b, c\ldots$ are different positive primes and the indices (α, α') $(\beta, \beta')\ldots$ are supposed not to be identical. Let $\alpha > \alpha'$: then

$$a^{\alpha-\alpha'} . b^\beta c^\gamma \ldots = b^{\beta'} c^{\gamma'} \ldots$$

that is $b^{\beta'} c^{\gamma'}\ldots$ is divisible by a, contrary to Cor. 2. Similarly if $\alpha' > \alpha$; therefore $\alpha' = \alpha$, and

$$b^\beta c^\gamma \ldots = b^{\beta'} c^{\gamma'} \ldots$$

A repetition of the argument gives $\beta = \beta'$, $\gamma = \gamma'$,... successively: so that the two resolutions are identical.

It should be observed that any even number of the factors of A may have their sign changed without altering the product: thus, for instance,

$$60 = 2^2 \,.\, 3 \,.\, 5 = (-2)^2 \,.\, 3 \,.\, 5 = 2^2 \,.\, (-3) \,.\, (-5) = \text{etc.}$$

but these resolutions are considered essentially the same, and this convention is understood in the statement of the theorem.

Similarly any negative composite number may be reduced to the form $(-1)\, a^\alpha b^\beta c^\gamma \ldots$ where a, b, $c\ldots$ are different positive primes, and all other resolutions of the number into prime factors are essentially equivalent to this.

4. If a, b, $c\ldots$ are all prime to k, their product is also prime to k.

For no prime factor contained in a or b or $c\ldots$ is contained in k: therefore the product $abc\ldots$ contains no prime factor of k and is consequently prime to k.

5. If a, b, $c\ldots$ are prime to each other, and each divides k, then their product divides k.

For if any power of a prime, say p^π, occurs in the product $abc\ldots$, it must occur in one of the factors, in a, suppose: therefore k, which is a multiple of a, must have p^π for a factor: and similarly for any other power of a prime contained in $abc\ldots$. Hence k is divisible by the product.

6. If a is prime to b, and ak is divisible by b, then k is a multiple of b.

For ak is divisible by b, and also by a: hence, by Art. 5, ak is divisible by ab, that is, $\frac{ak}{ab}$ or $\frac{k}{b}$ is an integer.

The function $\phi(n)$.

7. Let n be any positive integer, and let $\phi(n)$ denote the number of positive integers, 1 included, which are prime to n and not greater than n.

By definition $\phi(1) = 1$. Also if n is a prime number

$$\phi(n) = n - 1.$$

Next suppose n composite, and let p, q, r, $s\ldots$ be the different primes which divide n.

Consider the series of integers 1, 2, 3...n. Of these the following are multiples of p:

$$p,\ 2p,\ 3p, \dots \frac{n}{p}\cdot p$$

(n/p in all).

Write these down with the sign +.

Similarly write down all the multiples of q, r, s... each with the sign +.

In the same series there are $\dfrac{n}{pq}$ multiples of pq. Write these all down with the sign $-$: and do the same with all the multiples of pr, ps, qr... (taking all the products of p, q, r, s... two at a time).

Next write down all the multiples of the ternary products pqr, pqs..., each with the sign +, and so on: until at last we come to the multiples of $pqrs$... with the sign $(-)^{k-1}$, k being the number of different primes.

Now take any number θ which is not greater than n and not prime to it. It will involve in its composition a certain number (λ say) of the different primes p, q, r.... How many times will it occur among the multiples already written down? Evidently (taking its appearances in the order of the groups) λ times with the sign +, then $\dfrac{\lambda(\lambda-1)}{2}$ times with the sign $-$, then $\dfrac{\lambda(\lambda-1)(\lambda-2)}{3!}$ times with the sign +, and so on.

If then we take the algebraic sum of all the groups, we have θ occurring with a coefficient

$$\lambda - \frac{\lambda(\lambda-1)}{2!} + \frac{\lambda(\lambda-1)(\lambda-2)}{3!} - \dots = 1 - (1-1)^{\lambda} = 1.$$

Thus the algebraic sum in question is the sum of all positive integers not greater than n and not prime to it. Now the *number* of these integers is equal to the excess of the number of positive terms in the whole sum, as originally written, above the number of negative terms: that is, it is

$$n\left\{\left(\frac{1}{p}+\frac{1}{q}+\frac{1}{r}+\dots\right)-\left(\frac{1}{pq}+\frac{1}{pr}+\frac{1}{qr}+\dots\right)+\left(\frac{1}{pqr}+\frac{1}{pqs}+\dots\right)-\dots \right.$$
$$\left. \dots + (-1)^{k-1}\cdot\frac{1}{pqrs\dots}\right\}.$$

Subtracting this from n, we have finally

$$\phi(n) = n\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\left(1-\frac{1}{r}\right)\dots$$

Corollary 1. $\phi(p^{\alpha}) = p^{\alpha}\left(1 - \frac{1}{p}\right) = p^{\alpha-1}(p-1)$.

Corollary 2. If m is prime to m',

$$\phi(mm') = \phi(m) \,.\, \phi(m').$$

For let $p, q, r\dots$ be the different primes which divide m, and $p', q', r'\dots$ those which divide m'. Then

$$\begin{aligned}\phi(m) \,.\, \phi(m') &= m\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\left(1-\frac{1}{r}\right)\dots\\ &\quad\times m'\left(1-\frac{1}{p'}\right)\left(1-\frac{1}{q'}\right)\dots\\ &= mm'\left(1-\frac{1}{p}\right)\left(1-\frac{1}{q}\right)\dots\left(1-\frac{1}{p'}\right)\left(1-\frac{1}{q'}\right)\dots\\ &= \phi(mm'):\end{aligned}$$

observing that none of the primes $p, q, r\dots$ can be found in the set $p', q', r'\dots$.

It is not difficult to prove Corollaries 1 and 2 independently, and thence to deduce the main proposition. This is the method adopted by Gauss (*Disquisitiones Arithmeticæ*, Art. 38).

8. If $d, d', d''\dots$ are all the divisors of n (1 and n inclusive) then

$$\phi(d) + \phi(d') + \phi(d'') + \dots = n.$$

Resolve n into its prime factors, so that $n = a^{\alpha}b^{\beta}c^{\gamma}\dots$.

Then any divisor of n is of the form

$$\overset{\lambda}{a}\; b^{\mu}c^{\nu}\dots \;(\alpha \nless \lambda \nless 0, \text{ etc.})$$

so that

$$\begin{aligned}\Sigma\phi(d) = \Sigma\phi(a^{\lambda}b^{\mu}c^{\nu}\dots) &= \Sigma\phi(a^{\lambda}) \,.\, \phi(b^{\mu}) \,.\, \phi(c^{\nu})\dots\\ &= \{1 + \phi(a) + \phi(a^2) + \dots + \phi(a^{\alpha})\}\\ &\quad\times \{1 + \phi(b) + \phi(b^2) + \dots + \phi(b^{\beta})\}\\ &\quad\times \{1 + \phi(c) + \phi(c^2) + \dots + \phi(c^{\gamma})\} \times \dots\\ = \{1 + (a-1) + a(a-1) + \dots + a^{\alpha-1}(a-1)\}&\\ \times \{1 + (b-1) + b(b-1) + \dots + b^{\beta-1}(b-1)\} \times \dots&\\ = a^{\alpha} \,.\, b^{\beta} \,.\, c^{\gamma}\dots = n.&\end{aligned}$$

(For another proof, see Gauss, *D. A.* Art. 39.)

Congruences.

9. If the difference of two integers b and c is divisible by m, b and c are said to be congruent (or congruous) with respect to the modulus m, and this is expressed in writing by

$$b \equiv c \pmod{m}.$$

This is clearly the same thing as $c \equiv b \pmod{m}$. Each of the numbers b, c is said to be a residue (mod m) of the other. With respect to a given modulus, every number b has an infinite number of residues which are included in the expression $b + \lambda m$, λ being any integer.

In all that follows the modulus is supposed to be positive.

Any number is congruent (mod m) to one, and one only, of the numbers $0, 1, 2 \ldots (m-1)$: or again to one, and one only, of the series $0, -1, -2, \ldots -(m-1)$. These may be called a complete series of least residues, positive and negative respectively.

For a given number there will, generally speaking, be one and only one residue numerically less than $\frac{m}{2}$: this is called the absolutely least residue of the number. If m is even there will be a possible residue $\frac{m}{2}$, which is equivalent to $-\frac{m}{2}$: the complete system of absolutely least residues may be taken to be

$$0, \pm 1, \pm 2 \ldots \pm \frac{m-2}{2}, \frac{m}{2}:$$

while if m is odd, the absolutely least residues are given by

$$0, \pm 1, \pm 2 \ldots \pm \frac{m-1}{2}.$$

10. The following propositions are fundamental in the theory of congruences: most of them are so obvious as not to require a formal proof.

I. If $a \equiv b \pmod{m}$, and $a \equiv c \pmod{m}$,

then $$b \equiv c \pmod{m}.$$

II. If $a \equiv a'$, $b \equiv b'$, $c \equiv c'$, etc. (mod m),

then $$a \pm b \pm c \pm \ldots \equiv a' \pm b' \pm c' \pm \ldots \pmod{m}.$$

III. If $a \equiv a' \pmod{m}$,

then $$ka \equiv ka' \pmod{m}.$$

IV. If $a \equiv a'$ and $b \equiv b'$ (mod m),

then $$ab \equiv a'b' \pmod{m}.$$

For by III. $$ab \equiv a'b \equiv a'b'.$$

V. If $a \equiv a'$, $b \equiv b'$, $c \equiv c'$, etc. (mod m),

then $$abc \ldots \equiv a'b'c' \ldots \pmod{m}.$$

Proved by repeated application of IV.

Hence if $$a \equiv a' \pmod{m},$$ $$a^k \equiv a'^k \pmod{m},$$
k being a positive integer.

Finally, if $a \equiv a'$, $b \equiv b'$, $c \equiv c'$,... (mod m) and ϕ denote a rational integral function,

$$\phi(a, b, c \ldots) \equiv \phi(a', b', c', \ldots) \pmod{m}.$$

All the above propositions are precisely analogous to the corresponding theorems for ordinary equations: but there is one case not yet considered where the analogy ceases to hold good. Namely from the equation $ka = ka'$ we infer that, if k is neither zero nor infinite, $a = a'$: but from the congruence $ka \equiv ka'$ (mod m) we *cannot* infer that $a \equiv a'$ (mod m) unless k is prime to m. The legitimate inference is contained in the following theorem.

VI. If $ka \equiv kb$ (mod m),

then $$a \equiv b \pmod{m/d},$$
where d is the greatest common measure of k and m.

For suppose $k = k'd$, $m = m'd$, where k' is prime to m'. Then $(ka - kb)/m = k'd(a - b)/m'd = k'(a - b)/m'$: and since k' is prime to m', $a - b$ must be a multiple of m': that is, $a \equiv b$ (mod m'), or, which is the same thing, $a \equiv b$ (mod m/d).

11. Consider the congruence

$$ax^n + bx^{n-1} + \ldots + l \equiv 0 \pmod{m},$$

where $a, b, c \ldots l$ are given numbers and x is undetermined. Any integral value of x which satisfies the congruence may be called a root of the congruence.

The coefficients $a, b, c \ldots l$ may be replaced by any other coefficients which are congruent to them, and in particular by their least residues, without affecting the meaning of the congruence.

If ξ is any value of x which satisfies the congruence, any one of its residues (mod m) will also satisfy it. It is convenient to say that *one* solution is given by $x \equiv \xi \pmod{m}$, or that the congruence has *one* root $x \equiv \xi \pmod{m}$.

If p is a prime, the congruence

$$f(x) = ax^n + bx^{n-1} + \ldots + l \equiv 0 \pmod{p}$$

cannot have more than n incongruent roots.

For if α be any numerical quantity whatever,

$$f(x) = (x - \alpha) f_1(x) + f(\alpha)$$

identically: $f_1(x)$ being a polynomial of degree $(n-1)$.

Now suppose α an integer such that

$$f(\alpha) \equiv 0 \pmod{p}.$$

Then $$f(x) \equiv (x - \alpha) f_1(x) \pmod{p},$$

independently of x.

Let β be another root of the congruence: then putting $x = \beta$, we get

$$(\beta - \alpha) f_1(\beta) \equiv f(\beta) \equiv 0 \pmod{p},$$

and therefore, since β is supposed incongruent to α,

$$f_1(\beta) \equiv 0 \pmod{p}.$$

It follows as before that a polynomial $f_2(x)$ can be found, such that

$$f_1(x) \equiv (x - \beta) f_2(x) \pmod{p},$$

independently of x: and so on. If then the congruence has n incongruent roots $\alpha, \beta, \gamma \ldots \lambda$,

$$f(x) \equiv a(x - \alpha)(x - \beta) \ldots (x - \lambda) \pmod{p},$$

independently of x: i.e. this is an "identical" or "indeterminate" congruence.

Now let θ be any integer not congruent to any of the numbers $\alpha, \beta, \gamma \ldots \lambda$: then $f(\theta) \equiv a(\theta - \alpha)(\theta - \beta) \ldots (\theta - \lambda) \pmod{p}$. None of the factors on the right is a multiple of p: therefore, since p is prime, their product is prime to p: consequently $f(\theta)$ is prime to p, and $f(x) \equiv 0$ cannot have any roots distinct from $\alpha, \beta, \gamma \ldots \lambda$.

Observe that it is not proved that the congruence actually has n roots: in fact, this will not generally be the case.

If a congruence of the nth degree is satisfied by more than n incongruent values of the variable, it must be an identical congruence: the modulus being supposed prime, as above.

Linear Congruences.

12. Every linear congruence with one unknown quantity can be reduced to the form

$$ax \equiv b \pmod{m}.$$

Suppose in the first place that a is prime to m. Then if the numbers $0, 1, 2 \ldots (m-1)$ are each multiplied by a, the resulting products are all incongruent (mod m). For if two of them were congruent, say $ae \equiv af$, then $a(e-f) \equiv 0$; whence $e-f \equiv 0$, since a is prime to m: but this cannot be, because $e-f$ is less than m and different from zero. Hence the least positive residues of the products will be the numbers $0, 1, 2 \ldots (m-1)$, of course in a different order. For example, suppose $m = 12$, $a = 5$: then when

$$x = 0,\ 1,\ 2,\ 3,\ 4,\ 5,\ 6,\ 7,\ 8,\ 9,\ 10,\ 11$$
$$ax \equiv 0,\ 5,\ 10,\ 3,\ 8,\ 1,\ 6,\ 11,\ 4,\ 9,\ 2,\ 7.$$

Since the products form a complete system of residues, one and only one of them is congruent to b, hence the congruence $ax \equiv b$ has one and only one root.

For instance, to solve $5x + 11 \equiv 2 \pmod{12}$.

This gives $5x \equiv -9 \equiv 3$: and the preceding table shews that the solution of this is $x \equiv 3 \pmod{12}$.

When the modulus is large, this method becomes laborious, and it is necessary to find a more convenient practical method.

In the first place, the solution of $ax \equiv b$ may be deduced from that of $ax \equiv \pm 1$. Namely if $x \equiv \xi$ be the solution of the latter, then $x \equiv \pm b\xi$ is the solution of the former.

Now the congruence $ax \equiv \pm 1 \pmod{m}$ is equivalent to the indeterminate equation $ax - my = \pm 1$: and this can always be solved by reducing m/a to a continued fraction: namely, if p/q be the convergent immediately preceding m/a, $ap - mq = \pm 1$: so that the solution of $ax \equiv \pm 1$ is $x \equiv \pm p$ (where, of course, the signs do not necessarily correspond).

For example, to solve $365x \equiv 11 \pmod{1887}$ the work may be arranged as follows:

5	365	1887	5
7	55	62	1
6	6	7	1
		1	

The successive partial quotients being

$$5,\ 5,\ 1,\ 7,\ 1,\ 6,$$

the numerators of the convergents are

$$5 \quad 26 \quad 31 \quad 243 \quad 274 \quad 1887.$$

Since 274 comes in an odd place

$$365 \,.\, 274 \equiv -1 \pmod{1887}$$

and therefore the solution of the proposed congruence is

$$x \equiv -11 \,.\, 274 \equiv -3014$$
$$\equiv 760 \pmod{1887}.$$

Next suppose that a is not prime to m: and let d be the greatest common divisor of m and a. Then in order that the congruence may be possible, b must be a multiple of d: so that the given congruence is equivalent to

$$\frac{a}{d}x \equiv \frac{b}{d} \left(\text{mod } \frac{m}{d}\right).$$

This may be solved as already explained: and supposing that the solution is given by $x \equiv \xi \pmod{m/d}$, the original congruence has d roots

$$x \equiv \xi + \frac{km}{d} \pmod{m}.$$
$$(k = 0, 1, 2 \ldots (d-1)).$$

In the case of a composite modulus, it is sometimes convenient to proceed as follows.

Let the modulus $m = pq$, and the proposed congruence

$$ax \equiv b \pmod{m},$$

where a may be supposed prime to m, and therefore to p and q.

Let the solution of $ax \equiv b \pmod{p}$ be $x \equiv \xi \pmod{p}$. Substitute $\xi + yp$ for x in the given congruence: thus $a\xi + ayp \equiv b \pmod{pq}$, or $ayp \equiv b - a\xi \pmod{pq}$. Now $b - a\xi$ is a multiple of $p, = b'p$ say: therefore $ay \equiv b' \pmod{q}$. Suppose the solution of this is $y \equiv \eta \pmod{q}$: then that of the original congruence is $x \equiv \xi + p\eta \pmod{m}$.

By repeated application of this process the solution of a congruence with a composite modulus may be made to depend on the solution of a set of congruences each with a prime modulus.

For example, consider the congruence already solved,

$$365x \equiv 11 \pmod{1887}.$$

Here $1887 = 3 . 17 . 37$: and starting with $365x \equiv 11 \pmod{37}$, which reduces to $-5x \equiv 11 \pmod{37}$, we find

$$x \equiv -\frac{11 + 2 . 37}{5} \equiv -17 \pmod{37}.$$

Put $x = 37y - 17$: then

$$37 . 365y \equiv 17 . 365 + 11 \equiv 6216 \pmod{1887},$$

$$\therefore \quad 365y \equiv 168 \pmod{51}$$

whence $$8y \equiv 15 \pmod{51},$$

$$\therefore \quad y \equiv 0 \pmod{3} \text{ or } y = 3z \text{ say,}$$

where $$8z \equiv 5 \pmod{17},$$

$$\therefore \quad z \equiv 7 \pmod{17},$$

and thence successively $$y \equiv 21 \pmod{51},$$

$$x \equiv 37 . 21 - 17 \pmod{1887}$$

$$\equiv 760 \pmod{1887}.$$

13. A good illustration of the preceding methods is afforded by the problem of finding a number having given residues $a_1, a_2 \ldots a_r$ with respect to the given moduli $m_1, m_2 \ldots m_r$.

Let $p, q, r \ldots$ be the different primes which are factors of one or more of the moduli, and let

$$m = p^\alpha q^\beta r^\gamma \ldots$$

be the least common multiple of $m_1, m_2 \ldots m_r$.

Then p^α is a factor of one modulus at least, and no higher power of p divides any other modulus.

Suppose $m_i \equiv 0 \pmod{p^\alpha}$: then the required number (x) must $\equiv a_i \pmod{p^\alpha}$, and if any other modulus $m_{i'}$ contain a factor $p^{\alpha'}$, it is necessary that $a_{i'} \equiv a_i \pmod{p^{\alpha'}}$.

Similarly if $q^\beta, r^\gamma \ldots$ are contained in $m_j, m_k \ldots$

$$x \equiv a_j \pmod{q^\beta}, \quad \equiv a_k \pmod{r^\gamma}, \text{ etc.}$$

with a set of conditions similar to that above written, in order that the given congruences may be consistent.

Now let $\xi_i, \xi_j, \xi_k \ldots$ be numbers such that

$$\frac{m}{p^\alpha} . \xi_i \equiv 1 \pmod{p^\alpha},$$

$$\frac{m}{q^\beta} . \xi_j \equiv 1 \pmod{q^\beta},$$

and so on: then a suitable value for x will be

$$x = \frac{m}{p^\alpha} . a_i\xi_i + \frac{m}{q^\beta} . a_j\xi_j + \frac{m}{r^\gamma} a_k\xi_k + \ldots$$

For it is clear that

$$x \equiv \frac{m}{p^\alpha} \cdot a_i \xi_i \pmod{p^\alpha}$$

$$\equiv a_i \pmod{p^\alpha},$$

and similarly $$x \equiv a_j \pmod{q^\beta}, \text{ etc.}$$

If this value of x be called ω, all the admissible values of x are given by $x \equiv \omega \pmod{m}$.

14. Let A, B, C... be any integers, and let M be their greatest common divisor: then it is always possible to find integers α, β, γ... such that

$$\alpha A + \beta B + \gamma C + \ldots = M.$$

For let M_1 be the highest common divisor of A and B, so that $A = M_1 A'$, $B = M_1 B'$. Then we can find integers x, y such that $xA' + yB' = 1$: namely by solving the congruence $A'x \equiv 1 \pmod{B'}$, which can always be done, because A' is prime to B'.

Hence $$xA + yB = M_1(xA' + yB') = M_1.$$

Now let M_2 be the greatest common divisor of M_1 and C: then we can find integers x', y' such that

$$M_2 = x'M_1 + y'C = x'xA + x'yB + y'C.$$

It is clear that M_2 is the greatest common divisor of A, B, C: so that the theorem is proved for three integers A, B, C; and by proceeding in the same way, we can prove it for any number of integers.

15. Consider a set of simultaneous linear congruences involving n unknown quantities:

$$\left.\begin{aligned} a_1x_1 + a_2x_2 + \ldots + a_nx_n &\equiv r_1 \pmod{m_1} \\ b_1x_1 + b_2x_2 + \ldots + b_nx_n &\equiv r_2 \pmod{m_2} \\ &\vdots \\ l_1x_1 + l_2x_2 + \ldots + l_nx_n &\equiv r_n \pmod{m_n} \end{aligned}\right\}.$$

Let m be the least common multiple of m_1, $m_2 \ldots m_n$: then the given set of congruences may be replaced by the equivalent set (cf. Art. 10),

$$\frac{m}{m_1} a_1x_1 + \frac{m}{m_1} a_2x_2 + \ldots + \frac{m}{m_1} a_nx_n \equiv \frac{m}{m_1} r_1 \pmod{m},$$

$$\frac{m}{m_2} b_1x_1 + \frac{m}{m_2} b_2x_2 + \ldots + \frac{m}{m_2} b_nx_n \equiv \frac{m}{m_2} r_2 \pmod{m}, \text{ etc.:}$$

so that there is no loss of generality if the modulus is supposed to be the same for all the congruences.

The principle of the following solution is to substitute for the given congruences an equivalent set involving respectively n, $(n-1)$, $(n-2)$,...2, 1 of the unknown quantities.

The two linear congruences $u \equiv 0$, $v \equiv 0$ are equivalent to $u \equiv 0$ and $u - kv \equiv 0$, provided k is an integer prime to the modulus: viz. from the congruences last written we infer successively $kv \equiv 0$, and thence $v \equiv 0$, since k is prime to m.

For simplicity take three variables x, y, z, and suppose the congruences to be

$$\left.\begin{array}{l} ax\ +by\ +cz\ \equiv d \\ a'x\ +b'y\ +c'z\ \equiv d' \pmod{m} \\ a''x+b''y+c''z\equiv d'' \end{array}\right\}\ldots\ldots\ldots\ldots\ldots(\text{i}).$$

Assume, also, for the present, that the coefficients a, a', a'' have no common divisor except 1. Then it is possible to find integers p, q, r so that $pa + qa' + ra'' = 1$.

Multiply the congruences (i) in order by p, q, r respectively and add: thus

$$x + (pb + qb' + rb'')\,y + (pc + qc' + rc'')\,z \equiv pd + qd' + rd'' \ldots (\text{ii}).$$

Now one at least of the integers p, q, r must be prime to m: suppose p is so: then if the first of the congruences (i) is replaced by (ii), we get a new set of three equivalent to those given. Eliminate x from the first and second, and from the first and third of the new set: thus the original set is replaced by three equivalent congruences of which the first is (ii), while the others are of the form

$$\begin{array}{l} ey\ +fz\ \equiv g \\ e'y+f'z\equiv g'. \end{array}$$

The process may now be repeated: and it is clear that the reasoning is quite general, and that we get finally a set of equivalent congruences of the character stated above.

Now solve the last congruence, which contains only one variable: substitute in the last but one, and solve for the unknown variable, and so on.

For example take the following, given by Gauss:—

$$\begin{array}{ll} (1) & 3x + 5y + \ \ z \equiv 4, \\ (2) & 2x + 3y + 2z \equiv 7 \pmod{12}, \\ (3) & 5x + \ \ y + 3z \equiv 6. \end{array}$$

Subtracting the second congruence from the first,

$$(4)\qquad x + 2y - z \equiv -3.$$

Eliminating x from (4), (2) and (3), (2) respectively,

$$(5)\qquad -\ \ y + 4z \equiv 1,$$

$$(6)\qquad -9y + 8z \equiv 9.$$

Combining (5) and (6),

$$8z \equiv 0.$$

Thus the original set is replaced by

$$\begin{array}{rl} x + 2y - \ \ z \equiv & -3 \\ -\ \ y + 4z \equiv & \ \ 1 \\ 8z \equiv & \ \ 0. \end{array}$$

The last of these gives

$$z \equiv \ 0,\ 3,\ 6,\ 9\ \ (\text{mod } 12):$$

and hence correspondingly

$$\begin{array}{l} y \equiv 11,\ 11,\ 11,\ 11, \\ x \equiv 11,\ \ \ 2,\ \ \ 5,\ \ \ 8. \end{array}$$

If the coefficients a, a', a'' have θ for their greatest common measure we can find integers p, q, r so that $pa + qa' + ra'' = \theta$, and the argument proceeds as before, except that instead of (ii) we have a congruence

$$\theta x + (pb + qb' + rb'')\,y + (pc + qc' + rc'')\,z \equiv pd + qd' + rd'',$$

and, as before, x may be legitimately eliminated from this and two of the three given congruences. The same thing may occur at any stage of the process.

Of course in the application of this method we may arrive at an insoluble congruence: namely, one in which the coefficients of the variables are all divisible by a factor of m which is not contained in the absolute term: the given system is then insoluble.

Fermat's Theorem.

16. *If p is a prime, and a any integer prime to p, then* $a^{p-1} \equiv 1$ (mod p).

The numbers a, $2a$, $3a$,...$(p-1)\,a$ are all incongruent to each other (mod p): their least positive residues are therefore 1, 2, 3...$(p-1)$ in a certain order: consequently

$$a \,.\, 2a \,.\, 3a \ldots (p-1)\,a \equiv 1 \,.\, 2 \,.\, 3 \ldots (p-1)\quad (\text{mod } p).$$

Dividing both sides by $(p-1)\,!$, which is prime to p, we get

$$a^{p-1} \equiv 1\ (\text{mod } p).$$

This very important and beautiful theorem may be generalized, so as to include the case of a composite modulus. The more general statement of the theorem is as follows:—

If a is any integer prime to m, then $a^{\phi(m)} \equiv 1 \pmod{m}$.

The proof is exactly similar to that of the original theorem. Namely, if $\alpha, \beta, \gamma, \ldots \lambda$ are the $\phi(m)$ numbers which are less than m and prime to it, the products $a\alpha, a\beta, a\gamma \ldots a\lambda$ are all prime to m: moreover no two of them are congruent (mod m): for instance $a\alpha \equiv a\beta$ would give $a(\alpha - \beta) \equiv 0$, and thence $\alpha \equiv \beta$, which is absurd, since α, β are both less than m. Hence, as above, the products $a\alpha, a\beta, \ldots$ are congruent to $\alpha, \beta, \gamma \ldots \lambda$ in a different order: and therefore

$$a\alpha \,.\, a\beta \,.\, a\gamma \ldots a\lambda \equiv \alpha\beta\gamma \ldots \lambda.$$

Dividing by $\alpha\beta\gamma \ldots \lambda$, which is prime to m, we obtain

$$a^{\phi(m)} \equiv 1 \pmod{m}.$$

Wilson's Theorem.

17. Returning to the case of a prime modulus, it will be seen that Fermat's Theorem is equivalent to the statement that the congruence $x^{p-1} - 1 \equiv 0 \pmod{p}$ has exactly $(p-1)$ incongruent roots, viz. $x \equiv 1, 2, \ldots (p-1)$ respectively; hence, by Art. 11, the congruence

$$x^{p-1} - 1 \equiv (x-1)(x-2) \ldots (x-p+1) \pmod{p}$$

is an identical congruence. Putting $x = 0$, we infer that when p is an uneven prime

$$-1 \equiv (p-1)! \pmod{p}.$$

This remarkable result is known as Wilson's Theorem. It should be observed that the congruence last written is true *only* when p is a prime: for if p is composite, $(p-1)!$ must involve one at least of the prime factors of p, and therefore cannot $\equiv -1 \pmod{p}$.

An independent proof of Wilson's Theorem may be given. Let a be any number less than p and positive: then the congruence $ax \equiv 1 \pmod{p}$ can be satisfied by one and only one value of x which is positive and less than p. Let this be a', so that $aa' \equiv 1 \pmod{p}$. Generally speaking, a' is distinct from a: for the congruence $a^2 \equiv 1 \pmod{p}$, or $(a-1)(a+1) \equiv 0 \pmod{p}$, gives $a = 1$ or $(p-1)$. Hence the numbers $2, 3, 4 \ldots (p-2)$ can be distributed into pairs $(a, a')(b, b')\ldots$ such that $aa' \equiv bb' \equiv \ldots \equiv 1$ (mod p). The numbers a, b being different, so also will be a' and b': for if $a' = b'$ it follows that $a \equiv b$, which is impossible, since a, b are both positive and less than p.

Hence the product

$$2.3.4\ldots(p-2) \equiv (aa')(bb')\ldots$$
$$\equiv 1 \pmod{p}.$$

Multiplying by $p-1$, we have

$$(p-1)! \equiv p - 1 \equiv -1 \pmod{p}.$$

Residues of Powers. Indices.

18. Let a be any number prime to the modulus m. Consider the series of numbers

$$1, a, a^2, a^3 \ldots\ldots a^{m-1}$$

composed of the successive powers of a. These are all prime to m: therefore their least positive residues are included in the series $1, 2, 3 \ldots (m-1)$. Since there are m numbers altogether, at least two of them must be congruent to each other: suppose $a^\mu \equiv a^\nu$ where $\mu > \nu$. Then $a^{\mu-\nu} \equiv 1$ or $a^t \equiv 1$ say, where t is positive and less than m.

Suppose f is the *least* positive exponent for which $a^f \equiv 1$ (mod m): then f is said to be the exponent to which a appertains (mod m).

The numbers $1, a, a^2, \ldots a^{f-1}$ are all incongruent. For if any two of them were congruent, say $a^p \equiv a^q$, where both p and q are less than f, it would follow that $a^{p\sim q} \equiv 1$ where $p \sim q$ is a positive integer less than f: this contradicts the definition of f.

Hence in the series

$$1, a, a^2, a^3, \ldots \textit{ad inf.}$$

the residues of the successive terms recur periodically, there being f residues in each period: and, generally, $a^h \equiv a^k$ (mod m) if $h \equiv k$ (mod f), and conversely.

For instance, suppose the least positive residue of 5^{1000} (mod 31) be required. We have $5^3 \equiv 125 \equiv 1$ (mod 31): and since $1000 \equiv 1$ (mod 3), $5^{1000} \equiv 5$ (mod 31).

It has already been proved that $a^{\phi(m)} \equiv 1$ (mod m): hence $\phi(m) \equiv 0$ (mod f), that is, the exponent to which a appertains is a divisor of $\phi(m)$.

This important result may be proved independently. It is clear in the first place that f cannot exceed $\phi(m)$, because there are only $\phi(m)$ numbers less than m and prime to it, and the numbers $1, a, a^2, \dots a^{f-1}$, are all incongruent and prime to m. If f is less than $\phi(m)$, there will be at least one number b less than m and prime to it, and not congruent to any of the numbers $1, a, a^2, \dots a^{f-1}$. Consider the series

$$b, ba, ba^2, \dots ba^{f-1}.$$

These are all incongruent (mod m): moreover none of them can be congruent to any of the former series. For if $ba^h \equiv a^k$, then $b \equiv a^{k-h}$ or $\equiv a^{f+k-h}$, according as k is greater or less than h: in each case, b is congruent to one of the first series, contrary to hypothesis. If all the numbers less than m and prime to it are congruent to some or other of the $2f$ numbers thus obtained, then $2f = \phi(m)$: if not, let c be one of those that remain, and form the series $c, ca, ca^2, \dots ca^{f-1}$: these are all incongruent to each other and to the first series. They are also incongruent to all of the second series: for if $ca^h \equiv ba^k$, $c \equiv ba^{k-h}$ or $\equiv ba^{f+k-h}$ according as k is greater or less than h: in either case c is congruent to a number belonging to the second system, and this is contrary to hypothesis.

If the least positive residues of the $3f$ numbers now obtained do not exhaust all the $\phi(m)$ numbers less than m and prime to it, take d, one of those that remain, and form the least positive residues of $d, da, da^2, \dots da^{f-1}$; and so on. It is clear that in this way the complete set of $\phi(m)$ residues must at last be exhausted, and since we get additional residues in sets of f at a time, $\phi(m)$ must be a multiple of f.

Fermat's Theorem may be immediately deduced from this: for, putting $\phi(m) = ef$,

$$a^{\phi(m)} = (a^f)^e \equiv 1^e \equiv 1 \pmod{m}.$$

19. Suppose now that the modulus is a prime number p. It has been proved that the exponent f to which any number appertains (mod p) is a divisor of $(p-1)$. The question arises: having given d any divisor of $(p-1)$, are there any numbers to which the exponent d belongs, and if so, how many such numbers are there?

Let $\psi(d)$ denote the number of integers, positive and less than p, to which the exponent d appertains. Suppose there is at least one such integer, a. Then all the numbers $a, a^2, a^3 \dots a^d$ are incongruent (mod p) and they are all roots of the congruence

$x^d \equiv 1 \pmod{p}$. Hence there are no other distinct roots of this congruence; otherwise it would have more than d incongruent roots. Now if we take a^k, where k involves a factor of d,—δ suppose,—we have $(a^k)^{d/\delta} = (a^d)^{k/\delta} \equiv 1$, where the exponent $d/\delta < d$: consequently d is not the exponent to which a^k appertains. On the other hand, if k is prime to d, and f is the exponent to which a^k appertains, $(a^k)^f \equiv 1 \pmod{p}$, therefore $kf \equiv 0 \pmod{d}$, whence $f \equiv 0 \pmod{d}$, since k is prime to d. The smallest admissible value of f is therefore d: moreover $(a^k)^d = (a^d)^k \equiv 1 \pmod{p}$: so that in fact d is the exponent to which a^k appertains. We thus obtain $\phi(d)$ numbers appertaining to the exponent d: but as it has not yet been proved that any such number as a actually exists, all that can be inferred at present is that $\psi(d) = \phi(d)$ or else $\psi(d) = 0$. But since every one of the numbers $1, 2, 3 \ldots (p-1)$ appertains to some exponent or other, and each exponent is a divisor of $(p-1)$, it follows that

$$\psi(d) + \psi(d') + \psi(d'') + \ldots = p - 1,$$

where $d, d', d'' \ldots$ are the different divisors of $(p-1)$. But it has already been proved that

$$\phi(d) + \phi(d') + \phi(d'') + \ldots = p - 1,$$

and therefore $\psi(d)$ can never be zero, but must always be equal to $\phi(d)$. Thus there are exactly $\phi(d)$ numbers positive and less than p which appertain to the exponent d.

In particular there are $\phi(p-1)$ such numbers which appertain to the exponent $(p-1)$. These numbers are called *primitive roots of p*.

20. On account of the great importance of primitive roots, it is desirable to give a practicable method by which they may be found. When one has been discovered, the others may be found, if required, without difficulty: namely, if g is any one primitive root, then the whole system of primitive roots consists of the least positive residues of $g, g^\alpha, g^\beta, \ldots g^\lambda$, where $1, \alpha, \beta, \ldots \lambda$ are the $\phi(p-1)$ numbers less than $(p-1)$ and prime to it.

The principle of the following method, which is due to Gauss (*D. A.* Art. 73), is to find a succession of integers appertaining to higher and higher exponents: it is clear that if this can be done a primitive rcot must at last be obtained.

Take any number prime to p (in practice 2 is the most convenient, as being the smallest): let this be a, and form the period of least positive residues of its powers[1]. If there are $(p-1)$ terms in the period, a is a primitive root. If not, suppose there are f terms in the period. Take any other number b not congruent to any power of a, and calculate its period. Suppose there are g terms in this period, where $g < p-1$: (otherwise b is a primitive root, and we need not continue). There are two cases to consider: either g is, or is not a multiple of f. Take the latter case first, and let m be the least common multiple of f and g. Then we may always put $m = f'g'$, where f', g' are prime to each other, and such that f' is a divisor of f, and g' a divisor of g. For let q be a prime divisor of m, and q^k the highest power of q contained in m. Then q^k must divide one or both of f and g: if it divides f but not g, take it as a factor of f': if it divides g but not f, take it as a factor of g': if it divides both f and g, take it as a factor of f' *or* g' (it does not matter which): and similarly for any other power of a prime contained in m.

Then evidently $a^{f/f'}$ appertains to the exponent f' and $b^{g/g'}$ to the exponent g': and therefore $a^{f/f'}.b^{g/g'}$ appertains to the exponent $f'g'$, that is, m. For suppose λ to be the exponent to which $a^{f/f'}.b^{g/g'}$ appertains: then $a^{\lambda f/f'}.b^{\lambda g/g'} \equiv 1 \pmod{p}$: this requires that $\lambda \equiv 0 \pmod{f'}$ and $\lambda \equiv 0 \pmod{g'}$, and since f' is prime to g' it follows that $\lambda \equiv 0 \pmod{f'g'}$, so that the smallest admissible value of λ is $f'g'$ or m.

Secondly, g may be a multiple of f. Then $g > f$, so that in this case, as in the other, we have succeeded in finding a number appertaining to a *higher* exponent than that to which a appertains.

The process may be continued, and since we get a higher exponent every time, we must at last arrive at a primitive root.

For example, to find a primitive root of 97.

Forming the period of the powers of 2, the least positive residues are

2	4	8	16	32	64	31	62	27	54
11	22	44	88	79	61	25	50	3	6
12	24	48	96	95	93	89	81	65	33
66	35	70	43	86	75	53	9	18	36
72	47	94	91	85	73	49	1		

$$f = 48.$$

[1] Of course, in doing this, multiples of p are rejected whenever an opportunity occurs.

(Observe that since $96 \equiv -1 \pmod{97}$ the second half of the residues is obtained by subtracting each of the first half from 97.)

The smallest number not contained among the preceding residues is 5, and on forming its period, we find it to be a primitive root.

Again suppose $p = 73$ (Gauss's example).

Let $a = 2$: the series of power-residues is

$$2 \quad 4 \quad 8 \quad 16 \quad 32 \quad 64 \quad 55 \quad 37 \quad 1$$

$$\therefore\ f = 9.$$

Put $b = 3$: the power-residues are

$$3 \quad 9 \quad 27 \quad 8 \quad 24 \quad 72 \quad 70 \quad 64 \quad 46 \quad 65 \quad 49 \quad 1$$

$$\therefore\ g = 12.$$

Thus
$$m = 36, \quad f' = 9, \quad g' = 4,$$
$$a^{f/f'} . b^{g/g'} = 2 . 3^3 = 54,$$
so that 54 appertains to the exponent 36.

Forming its period, and taking the number 5, not contained in it, this is found to be a primitive root.

21. Suppose that g is a primitive root of p: then since the least positive residues of $1, g, g^2 \dots g^{p-2}$ are the numbers $1, 2, 3 \dots (p-1)$ in a certain order, any number a which is prime to p must be congruent $(\text{mod } p)$ to some power of g. If $g^\alpha \equiv a$ $(\text{mod } p)$, α is called *the index of a to the base g*, and may be denoted by $\text{ind}_g a$. Evidently, to a given base, a has an infinite number of indices all congruent $(\text{mod } \overline{p-1})$: these are not considered to be distinct. It is sometimes convenient to consider the least positive value of α as the index of a (to the base g) *par excellence.*

These indices possess properties analogous to those of logarithms: it is obvious from the definition that

$$\left.\begin{aligned} \text{ind}\,(ab) &\equiv \text{ind}\, a + \text{ind}\, b \\ \text{ind}\, a^m &\equiv m\, \text{ind}\, a \\ \text{ind}\, \frac{a}{b} &\equiv \text{ind}\, a - \text{ind}\, b \\ \text{ind}\, 1 &\equiv 0 \end{aligned}\right\} (\text{mod } \overline{p-1}),$$

the indices in each congruence being supposed to refer to the same base.

It should be noticed that the index of any number depends upon the particular primitive root which is taken for a base. Suppose that g, h are different primitive roots of p, and let $\text{ind}_g h = \lambda$ so that $h \equiv g^\lambda \pmod{p}$: then if m is any number prime to p, and μ its index to base h, $m \equiv h^\mu \equiv g^{\lambda\mu} \pmod{p}$: so that $\text{ind}_g m \equiv \lambda\mu \equiv \text{ind}_g h \,.\, \text{ind}_h m \pmod{\overline{p-1}}$. In particular, putting $m = g$, $\text{ind}_g h \,.\, \text{ind}_h g \equiv 1 \pmod{\overline{p-1}}$.

A complete table of indices may be used to obtain the solution of the binomial congruence $ax^n \equiv b \pmod{p}$: namely this gives $\text{ind}\, a + n \,.\, \text{ind}\, x \equiv \text{ind}\, b \pmod{\overline{p-1}}$, a linear congruence to find $\text{ind}\, x$; $\text{ind}\, a$ and $\text{ind}\, b$ being given by the table. Then $\text{ind}\, x$ being known, another reference to the table gives x.

This method is of no direct theoretical interest, because a complete table of indices in fact contains a record of all the solutions of $x^n \equiv a \pmod{p}$; so that we are really only looking out a result already obtained by trial. The result, however, is valuable, indirectly, in connection with the further theory of binomial and other congruences.

22. Let f be the exponent to which a appertains: then $a^f \equiv 1 \equiv g^{p-1} \pmod{p}$, g denoting (as usual) a primitive root of p. Hence $f \,.\, \text{ind}\, a \equiv 0 \pmod{\overline{p-1}}$: so that $\text{ind}\, a = \frac{k}{f}(p-1)$, where k is some integer. Now k is always prime to f: for if not, suppose $k = mk'$, $f = mf'$, then $\frac{k}{f}(p-1) = \frac{k'}{f'}(p-1)$, and hence $a^{f'} \equiv g^{k'(p-1)} \equiv 1 \pmod{p}$, where $f' < f$: but this is impossible, since f is the exponent to which a appertains.

Hence whatever primitive root g may be, $(p-1)/f$ is the greatest common measure of $(p-1)$ and $\text{ind}_g a$.

Conversely if m is the greatest common measure of $(p-1)$ and $\text{ind}\, a$, $(p-1)/m$ is the exponent to which a appertains.

23. If p is a prime number greater than 3, the product of all the primitive roots of $p \equiv 1 \pmod{p}$.

For the primitive roots are congruent (mod p) to $g, g^\alpha, g^\beta \ldots g^\lambda$, where $1, \alpha, \beta \ldots \lambda$ are the numbers less than $(p-1)$ and prime to it. If k is less than $(p-1)$ and prime to it, so also is

$(p-1)-k$: hence the above series can be distributed into couples such as g^k, g^{p-1-k}: now $g^k \cdot g^{p-1-k} = g^{p-1} \equiv 1 \pmod{p}$, and therefore the product of all the primitive roots $\equiv 1 \pmod{p}$.

The only exception occurs when $k = p-1-k$, or $k = \frac{1}{2}(p-1)$ and is at the same time prime to $(p-1)$: but this can only occur when $\frac{1}{2}(p-1) = 1$, that is when $p = 3$.

24. Suppose $p - 1 = a^\alpha b^\beta c^\gamma \ldots l^\lambda$, where $a, b, c \ldots l$ are different primes. Let A be any number which appertains to the exponent a^α. Then

$$1 + A + A^2 + \ldots + A^{a^\alpha - 1} \equiv 0 \pmod{p}.$$

Also $$1 + A^a + A^{2a} + \ldots + A^{a^\alpha - a} = \frac{A^{a^\alpha} - 1}{A^a - 1} \equiv 0 \pmod{p}.$$

Now the sum of all the numbers, positive and less than p, which appertain to the exponent a^α is congruent (mod p) to

$$(1 + A + A^2 + \ldots + A^{a^\alpha - 1}) - (1 + A^a + A^{2a} + \ldots + A^{a^\alpha - a}),$$

and is therefore a multiple of p.

It is here supposed that $\alpha > 1$. If $\alpha = 1$, the sum in question is congruent to

$$A + A^2 + A^3 + \ldots + A^{a-1} \equiv -1 \pmod{p}.$$

Thus the sum of all the numbers, positive and less than p, which appertain to the exponent a^α is congruent to 0 or -1 (mod p) according as $\alpha > 1$ or $\alpha = 1$.

For the sake of brevity write $\phi(a^\alpha) = a'$, $\phi(b^\beta) = b', \ldots \phi(l^\lambda) = l'$: let $A_1 A_2 \ldots A_{a'}$ be the a' numbers which appertain to the exponent a^α, and so on. Then any number of the form

$$ABC \ldots L$$

will appertain to the exponent $a^\alpha b^\beta c^\gamma \ldots l^\lambda$, that is, to $(p-1)$: it is therefore congruent to a primitive root of p. If we expand the product

$$(A_1 + A_2 + \ldots + A_{a'})(B_1 + B_2 + \ldots + B_{b'}) \ldots (L_1 + L_2 + \ldots + L_{l'}),$$

we get a sum consisting of $\phi(p-1)$ terms, each of which is congruent to a primitive root of p. No two of these terms are congruent to each other: for suppose, if possible,

$$ABC \ldots L \equiv A'B'C' \ldots L' \pmod{p}.$$

Raise both sides to the power $b^\beta c^\gamma \dots l^\lambda$: thus since $B^{b^\beta} \equiv 1$ etc.,

$$A^{b^\beta c^\gamma \dots} \equiv A'^{b^\beta c^\gamma \dots} \pmod{p},$$

therefore $$b^\beta c^\gamma \dots \text{ind } A \equiv b^\beta c^\gamma \dots \text{ind } A' \pmod{\overline{p-1}},$$

and hence $$\text{ind } A \equiv \text{ind } A' \pmod{a^\alpha}.$$

Moreover since A and A' appertain to the exponent a^α,

$$\text{ind } A \equiv \text{ind } A' \equiv 0 \pmod{b^\beta c^\gamma \dots},$$

by Art. 22;

therefore finally, since a^α is prime to $b^\beta c^\gamma \dots l^\lambda$,

$$\text{ind } A \equiv \text{ind } A' \pmod{\overline{p-1}},$$

whence $$A \equiv A' \pmod{p}.$$

Similarly we could conclude that $B \equiv B'$, $C \equiv C'$,...$L \equiv L'$ (mod p); but any two terms of the expanded expression must have at least one pair of corresponding factors such as A, A' which are incongruent (mod p). Hence no two of the terms are congruent: so that the expression is congruent (mod p) to the sum of all the primitive roots of p.

Now if any one of the exponents $\alpha, \beta, \gamma \dots \lambda$ is greater than 1, that is, if any square number can be found which divides $(p-1)$, one of the factors of the expression

$$(A_1 + A_2 + \dots)(B_1 + B_2 + \dots)\dots(L_1 + L_2 + \dots) \equiv 0 \pmod{p},$$

so that in this case the sum of the primitive roots $\equiv 0$ (mod p). If, however, each exponent is 1, so that $p-1 = abc \dots l$, each factor $\equiv -1$ (mod p) and the sum of the primitive roots $\equiv (-1)^\mu$ (mod p), where μ is the number of different prime factors of $(p-1)$.

This theorem may be proved in a different manner as follows. Let $g_1, g_2 \dots$ be the different primitive roots of p. For convenience write $p - 1 = q$, and let $a, b, c \dots$ be the different primes which divide q. Then the same argument by which $\phi(m)$ was determined (Art. 7) shews that the primitive roots of p are the roots of the congruence

$$\frac{(x^q - 1)\,\Pi\,(x^{q/ab} - 1)\,.\,\Pi\,(x^{q/abcd} - 1)\dots}{\Pi\,(x^{q/a} - 1)\,.\,\Pi\,(x^{q/abc} - 1)\,\Pi\,(x^{q/abcde} - 1)\dots} \equiv 0 \pmod{p},$$

where $$\Pi\,(x^{q/a} - 1) = (x^{q/a} - 1)(x^{q/b} - 1)\dots$$

and similarly for the rest. The expression on the left-hand side of the congruence is a rational integral function of x of the degree $\phi(q)$. This may be proved with the help of de Moivre's theorem: for any linear factor of the denominator is of the form $x - e^{2s\pi i/q}$, where δ is a number less than q and not prime to it: and it follows, just as in Art. 7, that this factor occurs precisely as often in the numerator as in the denominator.

Now suppose that q has no square divisor, so that $q = abcd\ldots$: then it has to be shewn that the aforesaid polynomial is of the form $x^{\phi(q)} - (-1)^{\mu} x^{\phi(q)-1} + \ldots$ where μ is the number of different primes $a, b, c\ldots$. This is easily proved by induction. Namely beginning with $\mu = 1$, we have

$$\frac{x^a - 1}{x - 1} = x^{a-1} + x^{a-2} + \ldots:$$

next when $\mu = 2$

$$\frac{(x^{ab}-1)(x-1)}{(x^a-1)(x^b-1)} = \frac{(x^b)^a - 1}{x^b - 1} : \frac{x^a - 1}{x - 1}$$
$$= (x^{ab-b} + x^{ab-2b} + \ldots) : (x^{a-1} + x^{a-2} + \ldots)$$
$$= x^{\phi(ab)} - x^{\phi(ab)-1} + \ldots.$$

This is seen by performing the first two steps of the actual division and observing that since $b > 1$

$$ab - 2b < ab - b - 1.$$

When $\mu = 3$, the function is

$$\frac{(x^{abc}-1)(x^a-1)(x^b-1)(x^c-1)}{(x^{bc}-1)(x^{ca}-1)(x^{ab}-1)(x-1)}$$
$$= \frac{\{(x^c)^{ab}-1\}\{x^c-1\}}{\{(x^c)^b-1\}\{(x^c)^a-1\}} : \frac{(x^{ab}-1)(x-1)}{(x^a-1)(x^b-1)},$$

and by the preceding case this is

$$(x^{c\phi(ab)} - x^{c\phi(ab)-c} + \ldots) : (x^{\phi(ab)} - x^{\phi(ab)-1} + \ldots) = x^{\phi(abc)} + x^{\phi(abc)-1} + \ldots,$$

the argument being as before. It is clear that the reasoning is quite general, so that in all cases the polynomial is

$$x^{\phi(q)} + (-1)^{\mu-1} x^{\phi(q)-1} + \ldots$$

Since this is identically congruent to $\Pi(x - g_i)$, the coefficients of $x^{\phi(q)-1}$ in the two expressions are congruent: that is

$$\Sigma g_i \equiv -(-1)^{\mu-1}$$
$$\equiv (-1)^{\mu} \pmod{p}.$$

If q involves a square factor, we shall have $q = m \,.\, abc\ldots$, and everything is as before except that the polynomial is of the form

$$x^{\phi(q)} + (-1)^{\mu-1} \,.\, x^{\phi(q)-m} + \ldots,$$

where the term in $x^{\phi(q)-1}$ is absent: so that in this case

$$\Sigma g_i \equiv 0 \pmod{p}.$$

It may be observed also that

$$\Sigma g^2 \equiv \Sigma g^3 \equiv \ldots \equiv \Sigma g^{m-1} \equiv 0 \pmod{p},$$

$$\Sigma g^m \equiv (-1)^\mu \,.\, m \pmod{p}.$$

For example, the primitive roots of 61 are 2 6, 7, 10, 17, 18, 26, 30, 31, 35, 43, 44, 51, 54, 55, 59. Here $q = 60 = 2^2 \,.\, 3 \,.\, 5$, so that $\mu = 3$, $m = 2$, and we ought to have $\Sigma g \equiv 0$, $\Sigma g^2 \equiv -2 \pmod{61}$; this may be easily verified.

25. It has been proved that if a is any number prime to the composite modulus m, $a^{\phi(m)} \equiv 1 \pmod{m}$. If $\phi(m)$ is the exponent to which a appertains (mod m), a is said to be a primitive root of m. It is only in a comparatively small number of cases that such primitive roots exist. For suppose $m = p^\lambda q^\mu r^\nu \ldots$ where $p, q, r \ldots$ are different primes. Any number, a, which is prime to m is also prime to $p^\lambda, q^\mu, r^\nu \ldots$: let $f, g, h \ldots$ be the exponents to which a appertains with respect to the moduli p^λ, q^μ, r^ν, etc.: so that

$$a^f \equiv 1 \pmod{p^\lambda},\ a^g \equiv 1 \pmod{q^\mu}, \text{ etc.}$$

Then if t is the least common multiple of $f, g, h \ldots$

$$a^t \equiv 1 \pmod{m}.$$

Now the greatest possible values of $f, g, h \ldots$ are $\phi(p^\lambda)$, $\phi(q^\mu)$, $\phi(r^\nu) \ldots$: hence t is not greater than the L.C.M. of $\phi(p^\lambda)$, $\phi(q^\mu)$, etc., and if it is less than this L.C.M. it must be a divisor thereof (since f is a factor of $\phi(p^\lambda)$, etc. by Art. 18). Again

$$\phi(p^\lambda) = (p-1)\,p^{\lambda-1},$$

which is an even number, except when $p = 2$ and $\lambda = 1$. Hence, generally speaking, the L.C.M. of $\phi(p^\lambda)$, $\phi(q^\mu)$, etc. will be less than $\phi(p^\lambda) \,.\, \phi(q^\mu) \ldots$, i.e. less than $\phi(m)$, and *a fortiori* t will be less than $\phi(m)$, so that a cannot be a primitive root. The only exceptions are when m is a power of a prime, or twice a power of an uneven prime.

Further the case of $m = 2^\lambda$ has to be rejected if $\lambda > 2$. For any odd number can be expressed in the form

$$a = 1 + 2k,$$

whence

$$\begin{aligned} a^2 = 1 + 4(k^2 + k) &= 1 + 4k(k+1) \\ &\equiv 1 \pmod{8}, \end{aligned}$$

and therefore, successively

$$a^4 \equiv 1 \pmod{16},$$

$$a^8 \equiv 1 \pmod{32},$$

and generally

$$a^{2^{\lambda-2}} \equiv 1 \pmod{2^\lambda}.$$

Now $$2^{\lambda-2} < 2^{\lambda-1} < \phi(2^\lambda),$$

so that 2^λ has no primitive roots if $\lambda > 2$.

26. The only cases which have to be considered are therefore when $m = p^\lambda$ or $2p^\lambda$ where p is an odd prime, and the exceptional case of $m = 4$.

The last case is easily disposed of: it is evident that there is one primitive root, viz. 3.

Next let $m = p^\lambda$. Suppose a is any number prime to m and therefore to p, and let f be the exponent to which a appertains (mod p). Then

$$a^f = 1 + kp.$$

Hence
$$\begin{aligned} a^{fp} &= (1+kp)^p \\ &= 1 + kp \,.\, p + k^2p^2 \,.\, \frac{p(p-1)}{2} + \dots \\ &\equiv 1 \pmod{p^2}, \end{aligned}$$

and similarly,

$$\begin{aligned} &a^{fp^2} = (a^{fp})^p \equiv 1 \pmod{p^3}, \\ &\vdots \\ &a^{fp^{\lambda-1}} \equiv 1 \pmod{p^\lambda}. \end{aligned}$$

If, then, a is to be a primitive root of p^λ we must have $fp^{\lambda-1}$ a multiple of $\phi(p^\lambda)$, i.e. of $(p-1)p^{\lambda-1}$: hence f is a multiple of $(p-1)$.

But f is also a divisor of $(p-1)$ by Art. 18: hence

$$f = p - 1,$$

that is, a is a primitive root of p.

Suppose, then, we put $a = g$, a primitive root of p; then

$$g^{p-1} = 1 + kp^i,$$

p^i being the highest power of p which divides $g^{p-1} - 1$, so that k is prime to p. Raising each side to the power p we infer that

$$\begin{aligned} g^{(p-1)p} &= 1 + kp^i \,.\, p + \frac{p(p-1)}{2}(kp^i)^2 + \dots \\ &= 1 + kp^{i+1} + \text{higher powers of } p \\ &\equiv 1 + kp^{i+1} \pmod{p^{i+2}}, \end{aligned}$$

and similarly

$$\begin{aligned} &g^{(p-1)p^2} \equiv 1 + kp^{i+2} \pmod{p^{i+3}}, \\ &\vdots \qquad \vdots \qquad \vdots \qquad \vdots \\ &g^{(p-2)p^h} \equiv 1 + kp^{i+h} \pmod{p^{i+h+1}}. \end{aligned}$$

Putting $h = \lambda - i$, we have

$$g^{(p-1)p^{\lambda-i}} \equiv 1 \pmod{p^\lambda},$$

so that g is a primitive root of p^λ if, and only if $i = 1$; that is, if $(g^{p-1} - 1)/p$ is prime to p.

27. It remains to find the number of distinct primitive roots of p^λ: i.e. the number of such roots which are positive and less than p^λ. Any primitive root of this kind may be written

$$g = a + kp,$$

where a is a primitive root of p which is positive and less than p.

Hence

$$\begin{aligned} g^{p-1} - 1 &\equiv (a^{p-1} - 1) + kp\,(p-1)\,a^{p-2} \pmod{p^2} \\ &\equiv (a^{p-1} - 1) - kpa^{p-2} \pmod{p^2}. \end{aligned}$$

There are two cases to consider:

I. Suppose $a^{p-1} - 1 \equiv 0 \pmod{p^2}$: then

$$g^{p-1} - 1 \equiv -kpa^{p-2} \pmod{p^2},$$

$$\therefore\ (g^{p-1} - 1)/p \equiv -ka^{p-2} \pmod{p},$$

and this will be prime to p if k is so.

Now since $g < p^\lambda$, $k < p^{\lambda-1}$: thus we obtain $\phi(p^{\lambda-1})$ suitable values for g by assigning to k the $\phi(p^{\lambda-1})$ values which are less than $p^{\lambda-1}$ and prime to it.

II. Suppose $a^{p-1} - 1$ is not divisible by p^2: then we may put

$$a^{p-1} - 1 \equiv hp \pmod{p^2},$$

where h is positive, less than p and prime to p. This gives

$$g^{p-1} - 1 \equiv hp - kpa^{p-2} \pmod{p^2},$$

or

$$\frac{g^{p-1} - 1}{p} \equiv h - ka^{p-2} \pmod{p}.$$

Multiplying by a, which is prime to p, and observing that $a^{p-1} \equiv 1 \pmod{p}$,

$$\frac{g^{p-1} - 1}{p} \,.\, a \equiv ha - k \pmod{p}.$$

The necessary condition will be satisfied if $ha - k$ is prime to p: that is, if $k = ha + l$, where l is prime to p.

As in the other case we thus obtain $\phi(p^{\lambda-1})$ suitable values for g.

Since there are $\phi(p-1)$ primitive roots of p which are less than p, the number of distinct primitive roots of p^λ is

$$\phi(p-1)\,.\,\phi(p^{\lambda-1}) \equiv \phi\,\{(p-1)\,p^{\lambda-1}\} = \phi\,\{\phi(p^\lambda)\}.$$

28. Now let the modulus $m = 2p^\lambda$, where p is an odd prime.

Every odd number appertains to the same exponent (mod $2p^\lambda$) as it does (mod p^λ). For let f be the exponent to which the odd number a appertains (mod p^λ): then $a^f \equiv 1$ (mod p^λ). Also since a is odd, $a^f \equiv 1$ (mod 2): hence, 2 being prime to p^λ, $a^f \equiv 1$ (mod $2p^\lambda$). Conversely, if $a^{f'} \equiv 1$ (mod $2p^\lambda$), $a^{f'} \equiv 1$ (mod p^λ): therefore a appertains to the same exponent in both cases.

Moreover $\phi(2p^\lambda) = \phi(2)\,\phi(p^\lambda) = \phi(p^\lambda)$: so that any odd primitive root of p^λ is also a primitive root of $2p^\lambda$. If g is an even primitive root of p^λ, $g + p^\lambda$ is odd and therefore a primitive root of $2p^\lambda$. We thus obtain just as many primitive roots of $2p^\lambda$ as of p^λ.

29. The modulus 2^λ, where $\lambda > 2$, requires separate consideration. Any odd number of the series $1, 3, 5 \ldots 2^\lambda - 1$, may be expressed in the form

$$a = 2^n k \pm 1,$$

where k is odd, and n is at least equal to 2.

Hence
$$\begin{aligned} a^2 &= 2^{2n}k^2 \pm 2^{n+1}k + 1 \\ &= 2^{n+1}k_1 + 1, \end{aligned}$$

where k_1 is odd: and similarly

$$\begin{aligned} a^4 &= 2^{n+2}k_2 + 1 \\ &\vdots \\ a^{2^t} &= 2^{n+t}k_t + 1, \end{aligned}$$

where $k_2, k_3 \ldots k_t$ are all odd.

The only number which appertains to the exponent 1 is 1.

If $a^2 \equiv 1$ (mod 2^λ), it follows from the preceding expression for a^2 that $n + 1 \not< \lambda$, that is, $n \not< \lambda - 1$; and it is easily seen that there are three admissible values of a, namely

$$2^\lambda - 1,\ 2^{\lambda-1} + 1,\ 2^{\lambda-1} - 1.$$

Next suppose a appertains to the exponent 2^t where $t > 1$: then $n + t \not< \lambda$, or $n \not< \lambda - t$. Moreover if n were greater than $\lambda - t$, say $n = \lambda - t + u$, we should have

$$\begin{aligned} a^{2^{t-u}} &= 2^{n+t-u} \,.\, k_{t-u} + 1 = 2^\lambda k_{t-u} + 1 \\ &\equiv 1 \pmod{2^\lambda}, \end{aligned}$$

i.e. a would not appertain to the exponent 2^t. Hence $n = \lambda - t$, and therefore the numbers appertaining to the exponent 2^t are

$$2^{\lambda-t} \pm 1,\quad 3\,.\,2^{\lambda-t} \pm 1,\quad 5\,.\,2^{\lambda-t} \pm 1, \ldots$$
$$(2^t - 1)\,.\,2^{\lambda-t} \pm 1 \ (2^t \text{ numbers in all}).$$

In particular, if $\lambda > 3$, the numbers appertaining to the exponent $2^{\lambda-2}$ (the highest possible, since $n > 1$) are

$$4 \pm 1, \quad 3 . 4 \pm 1, \quad 5 . 4 \pm 1, \ldots (2^{\lambda-2} - 1) 4 \pm 1.$$

These may be written

$$4 \pm 1, \quad 8 + (4 \pm 1), \quad 2 . 8 + (4 \pm 1), \ldots$$

from which it is evident that the series comprises all the numbers less than 2^{λ} which are of the form $8n + 3$ or $8n + 5$.

AUTHORITIES.

This chapter is substantially a paraphrase of the first three sections of the *Disquisitiones Arithmeticæ*. The invention of the symbol ≡ by Gauss affords a striking example of the advantages which may be derived from an appropriate notation, and marks an epoch in the development of the science of arithmetic. References to the work of Gauss's predecessors are given by himself (*D. A.* Arts. 28, 38, 44, 50, 56, 76, 93), and also by H. J. S. Smith in Arts. 1—14 of his Report on the Theory of Numbers (*Report of British Ass.* 1859). The most important of these, arranged according to the subjects treated, are the following:

Continued Fractions and Linear Congruences. Euler: *Solutio problematis arithmetici...* (Comment. Petropol. vii. p. 46 (1740), or Commentationes Arithmeticæ i. p. 11). Lagrange: *Sur la Solution des Problèmes Indéterminés du second degré* (Histoire de l'Acad. de Berlin 1767, p. 165), and in the additions to the French translation of Euler's Algebra. See also Smith, H. J. S.: *On Systems of Linear Indeterminate Equations and Congruences* (Phil. Trans. cli. (1861) p. 293).

The Function $\phi(n)$. Euler: *Theoremata arithmetica nova methodo demonstrata* (Comment. Nov. Petrop. viii. 74 (1760), or Comm. Arith. i. 274).

Sylvester writes $\tau(n)$ for $\phi(n)$, and calls it the *totient* of n. See two papers by him, Phil. Mag., April 1882, p. 251, and Sept. 1883, p. 230, containing tables of $\phi(n)$ and $\Sigma\phi(n)$ up to $n = 1000$.

Residues of Powers. Euler: *Theoremata circa residua ex divisione potestatum relicta* (Novi Comm. Petr. vii. (1758) p. 49); *Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia* (ibid. xviii. (1773) p. 85); *Disquisitio accuratior circa residua ex divisione quadratorum altiorumque potestatum per numeros primos relicta* (Opuscula analytica i. (1772) p. 121). These three memoirs may also be found in the Comm. Arith. i. pp. 260, 516, 487 respectively. It should be observed that Gauss first proved the existence of primitive roots for every prime modulus.

Theorems of Fermat and Wilson. Fermat's own statement of his theorem is contained in his mathematical correspondence (see Varia Opera

Mathematica D. Petri de Fermat (1679) p. 163). As usual, he gives no proof; the first published demonstration is that of Euler: *Theorematum quorundam ad numeros primos spectantium demonstratio* (Comm. Petr. viii. (1736) p. 141, or Comm. Arith. i. 21). This practically amounts to showing that if p is prime, the expression $(a+1)^p-a^p-1$, is identically divisible by p, so that $(a+1)^p-(a+1)\equiv a^p-a \pmod{p}$, identically: the theorem then follows by induction. A second proof, identical with that of Art. 18, will be found in the Novi Comm. Petr. vii. 49 (see title above). The proof adopted in Art. 16 is after Dirichlet: *Démonstrations nouvelles de quelques théorèmes relatifs aux nombres* (Crelle iii. (1828) p. 390). Sir John Wilson's theorem is stated by Waring, with a reference to its author, in his *Meditationes Algebraicæ* (1770); the first published proof is by Lagrange (Nouveaux Mémoires de l'Acad. de Berlin, 1771, p. 125).

The important theorem of Art. 11 is due to Lagrange: *Nouvelle Méthode pour résoudre les Problèmes Indéterminés en Nombres entiers* (Hist. de l'Acad. de Berlin, 1768, p. 192).

Arithmetical Tables. The factor-tables of Burckhardt and Dase have been completed and extended by J. W. L. Glaisher as far as the 9th million. The *Canon Arithmeticus*, edited by Jacobi, gives a primitive root, and a table of numbers and indices, for all primes less than 1000. Gauss's *Tafel zur Verwandlung gemeiner Brüche in Decimalbrüche* (Werke ii. 412) may be used, among other applications, to supply the place of the *Canon Arithmeticus*, at least as far as $p=463$. (Cf. *D. A.* Arts. 312—318.) Another table, of less extent, but very compact, is given by Bellavitis: *Sulla risoluzione delle congruenze numeriche...* (Reale Acc. dei Lincei, 3rd series, t. i. (1877)). Crelle published in his Journal (xlii. (1851) p. 299) a table of the least positive values of x_1 and x_2 which satisfy $a_1x_2=a_2x_1+1$ for values of a_1 up to 120 and all values of a_2 less than a_1 and prime to it.

CHAPTER II.

Quadratic Congruences.

30. If the congruence $x^2 \equiv a \pmod{m}$ is possible, a is said to be a quadratic residue of m, or simply a residue of m, and this may be indicated by writing aRm: if otherwise, a is said to be a non-residue of m, and this is expressed by aNm.

It is convenient to begin by supposing that the modulus is an odd prime, p say.

If we form the squares of $1, 2, 3 \ldots \frac{1}{2}(p-1)$, the resulting numbers are all incongruent (mod p). For if two of them were congruent, say $r^2 \equiv s^2$, this would give $(r+s)(r-s) \equiv 0$, that is, $r + s \equiv 0$, or $r - s \equiv 0$, both of which are impossible, since r and s are different and each less than $\frac{1}{2}p$.

Again since $(p-k)^2 \equiv k^2 \pmod{p}$, it follows that the squares of $\frac{p+1}{2}, \frac{p+3}{2} \ldots (p-1)$ are congruent to the other series of squares in the reverse order. Hence the series $1, 2, 3 \ldots (p-1)$ comprises $\frac{p-1}{2}$ residues of p, and the same number of non-residues.

For example if $p = 11$,

$$1^2 \equiv 10^2 \equiv 1,\ 2^2 \equiv 9^2 \equiv 4,\ 3^2 \equiv 8^2 \equiv 9,\ 4^2 \equiv 7^2 \equiv 5,\ 5^2 \equiv 6^2 \equiv 3,$$

so that 1, 3, 4, 5, 9 are residues of 11, and 2, 6, 7, 8, 10 are non-residues.

If aRp, so that $a \equiv x^2 \pmod{p}$,

$$a^{\frac{p-1}{2}} \equiv x^{p-1} \equiv 1 \pmod{p}.$$

Thus the quadratic residues of p are the roots of the congruence

$$x^{\frac{p-1}{2}} - 1 \equiv 0 \pmod{p}.$$

Every number prime to p satisfies the congruence

$$x^{p-1} - 1 \equiv 0,$$

that is $$(x^{\frac{p-1}{2}} - 1)(x^{\frac{p-1}{2}} + 1) \equiv 0,$$

hence the non-residues of p are the roots of the congruence

$$x^{\frac{p-1}{2}} + 1 \equiv 0.$$

This affords a method of determining whether a given number a is a residue or non-residue of p, namely by calculating the least residue of $a^{\frac{p-1}{2}}$: but this becomes impracticable when p is large.

As an illustration $5^5 = 5 \,.\, 25^2 \equiv 5 \,.\, 3^2 \equiv 45 \equiv 1 \pmod{11}$, so that 5 is a residue of 11.

The symbol $\left(\frac{a}{p}\right)$ or $(a \mid p)$ is used to denote $+1$ or -1 according as a is, or is not a quadratic residue of p. It is the absolutely least residue (mod p) of $a^{\frac{p-1}{2}}$.

31. The product of two residues or of two non-residues is a residue: that of a residue and a non-residue is a non-residue.

I. Let a, a' be two residues: then two integers α, α' can be found such that $a \equiv \alpha^2$, $a' \equiv \alpha'^2$, whence $aa' \equiv (\alpha\alpha')^2$, that is, aa' is a residue.

II. If a is a residue, the numbers $a, 2a, 3a \ldots (p-1)a$ are all incongruent, and their least residues (mod p) include all the quadratic residues of p and all the non-residues; but each product of a by a residue is a residue by I.: hence each product of a by a non-residue is a non-residue.

III. Let b be a non-residue: then as before the series $b, 2b, 3b, \ldots (p-1)b$ is a complete system of residues (mod p): each product of b by a residue is a non-residue by II.: hence each product of b by a non-residue is a residue.

The same thing may be proved as follows: we have

$$a^{\frac{p-1}{2}} \equiv (a \mid p),\ b^{\frac{p-1}{2}} \equiv (b \mid p),\ (ab \mid p) \equiv (ab)^{\frac{p-1}{2}} \equiv a^{\frac{p-1}{2}}\, b^{\frac{p-1}{2}} \equiv (a \mid p)(b \mid p).$$

Hence $(ab \mid p) = +1$ if $(a \mid p)$ and $(b \mid p)$ agree in sign, that is if a, b are both residues or both non-residues: while if one is a residue and the other not, $(ab \mid p) = -1$, that is, ab is a non-residue.

It is clear that
$$(abc\,|\,p) = (ab\,|\,p)(c\,|\,p)$$
$$= (a\,|\,p)(b\,|\,p)(c\,|\,p),$$
and so on for any number of factors.

32. Taking any primitive root of p for a base, the indices of the quadratic residues are even, and those of the non-residues are odd.

For let $\text{ind}_g\, a = f$: then $a \equiv g^f \pmod{p}$ and $a^{\frac{p-1}{2}} \equiv g^{\frac{f(p-1)}{2}}$: if then $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$, $\frac{1}{2}f(p-1) \equiv 0 \pmod{\overline{p-1}}$, that is $\frac{1}{2}f$ is an integer: conversely, if f is even and $= 2f'$, $a^{\frac{p-1}{2}} \equiv g^{f'(p-1)} \equiv 1 \pmod{p}$.

This gives another simple proof of the theorem of last article: for $\text{ind}\,(ab) = \text{ind}\, a + \text{ind}\, b$, and this is even if $\text{ind}\, a$ and $\text{ind}\, b$ are both even or both odd.

33. Consider the congruence
$$x^2 \equiv a \pmod{p^\lambda},$$
where p is an odd prime, and a is prime to p. Then if this is possible, so also is
$$x^2 \equiv a \pmod{p}.$$

Let $x \equiv \alpha$ be a solution of this last congruence, so that
$$\alpha^2 - a = hp.$$

Put
$$x = \alpha + yp:$$
then
$$x^2 - a = \alpha^2 - a + 2\alpha yp + y^2p^2$$
$$= (h + 2\alpha y)\, p + y^2p^2.$$

Now determine y so that $h + 2\alpha y \equiv 0 \pmod{p}$: then $x^2 - a \equiv 0 \pmod{p^2}$: that is, a solution of $x^2 \equiv a \pmod{p^2}$ can be deduced from that of $x^2 \equiv a \pmod{p}$.

More generally, from a solution of $x^2 \equiv a \pmod{p^\lambda}$ we can deduce a solution of $x^2 \equiv a \pmod{p^{\lambda+1}}$. For suppose $x = \alpha$ is a solution of $x^2 \equiv a \pmod{p^\lambda}$, so that $\alpha^2 - a = hp^\lambda$. Write $x = \alpha + yp^\lambda$: then $x^2 - a = (h + 2\alpha y)\, p^\lambda + y^2p^{2\lambda} \equiv (h + 2\alpha y)\, p^\lambda \pmod{p^{\lambda+1}}$: and hence if $2\alpha y + h \equiv 0 \pmod{p}$, $x = \alpha + yp^\lambda$ is a solution of $x^2 \equiv a \pmod{p^{\lambda+1}}$.

Thus from any solution of $x^2 \equiv a \pmod{p}$ can be deduced a solution of $x^2 \equiv a \pmod{p^\lambda}$. Moreover if $x^2 \equiv a \pmod{p}$ is possible, there are two distinct solutions of the form $x \equiv \alpha$ and $x \equiv -\alpha \pmod{p}$: so that there will be just two solutions of $x^2 \equiv a \pmod{p^\lambda}$.

For example, to solve $x^2 \equiv 2 \pmod{343}$. Here $2 \equiv 9 \pmod 7$: so that the roots of $x^2 \equiv 2 \pmod 7$ are $x \equiv \pm 3 \pmod 7$.

Write
$$x = 3 + 7y;$$
then
$$x^2 - 2 = 7(1 + 6y) + 49y^2.$$

The congruence $1 + 6y \equiv 0 \pmod 7$ gives $y \equiv 1 \pmod 7$: so that $x = 10$ is a solution of $x^2 \equiv 2 \pmod{49}$. Finally, putting $x = 10 + 49y$, $x^2 - 2 = 49(2 + 20y) + 49^2y^2$; $2 + 20y \equiv 0 \pmod 7$ gives $y \equiv 2 \pmod 7$, and hence $x = 10 + 2 . 49 = 108$ is a solution of the given congruence, the complete solution being
$$x \equiv \pm 108 \pmod{343}.$$

34. The case next to be considered is when the modulus is a power of 2.

The square of any odd number $2n + 1$ is
$$4n^2 + 4n + 1 = 4n(n + 1) + 1 \equiv 1 \pmod 8$$
since either n or $n + 1$ is even.

Hence in the first place the congruence $x^2 \equiv a \pmod 4$ is possible if, and only if $a \equiv 1 \pmod 4$: and if this condition is satisfied, there are two distinct solutions, given by $x \equiv \pm 1 \pmod 4$.

Similarly the congruence $x^2 \equiv a \pmod 8$ is possible only if $a \equiv 1 \pmod 8$: and in this case there are four distinct solutions given by $x \equiv 1, 3, 5, 7 \pmod 8$.

Next consider the congruence $x^2 \equiv a \pmod{2^\lambda}$ where $\lambda > 3$. This involves $x^2 \equiv a \pmod 8$: and hence $a \equiv 1 \pmod 8$: conversely if this condition is satisfied, it may be shewn by an inductive process similar to that of last article that the proposed congruence has always four distinct roots.

Namely, suppose α is a root of $x^2 \equiv a \pmod{2^\lambda}$ so that $\alpha^2 - a = 2^\lambda h$: then putting $x = \alpha + 2^{\lambda-1} . y$ we get
$$x^2 - a = 2^\lambda(h + \alpha y) + 2^{2\lambda-2}y^2$$
where since $\lambda > 3$, $2\lambda - 2 > \lambda + 1$: so that x will be a root of $x^2 - a \equiv 0 \pmod{2^{\lambda+1}}$ if $h + \alpha y \equiv 0 \pmod 2$: this always gives a suitable value of y, since α is odd.

If $x \equiv \xi$ is any one of the roots, it is easily seen that the four distinct solutions are given by
$$x \equiv \pm \xi,\ x \equiv \pm(\xi + 2^{\lambda-1}) \pmod{2^\lambda}.$$

35. We are now able to discuss the congruence $x^2 \equiv a \pmod{m}$ where m is any modulus whatever, and a any number prime to it.

Let $$m = 2^\kappa p^\lambda q^\mu r^\nu \dots$$

where $p, q, r \dots$ denote different odd primes.

Then if the proposed congruence is possible, so also must be the following:

$$x^2 \equiv a \pmod{2^\kappa},\ x^2 \equiv a \pmod{p^\lambda},\ x^2 \equiv a \pmod{q^\mu}$$

etc. Conversely if these are possible so is the given congruence. For suppose $\xi, \eta, \zeta \dots$ etc. to be any values of x which satisfy the congruences

$$x^2 \equiv a \pmod{2^\kappa},\ x^2 \equiv a \pmod{p^\lambda},\ x^2 \equiv a \pmod{q^\mu}, \dots$$

respectively. Then since $2^\kappa, p^\lambda, q^\mu \dots$ are relative primes, a number can be found so as to satisfy simultaneously the congruences

$$x \equiv \xi \pmod{2^\kappa},\ x \equiv \eta \pmod{p^\lambda},\ x \equiv \zeta \pmod{q^\mu} \dots \text{etc.}$$

and all such numbers are congruent (mod m) (see Art. 13). Each set of solutions of the auxiliary congruences furnishes therefore one distinct solution of the proposed congruence.

Now the conditions to be satisfied in order that the auxiliary congruences may be possible were determined in Arts. 33, 34. If p is any odd prime factor of m, a must be a quadratic residue of p: and if this is so, the congruence $x^2 \equiv a \pmod{p^\lambda}$ has two distinct roots. If $\kappa = 0$ or 1, there is no further condition: the congruence $x^2 \equiv a \pmod{2}$ has one root $x \equiv 1 \pmod{2}$: if $\kappa = 2$ it is necessary that $a \equiv 1 \pmod{4}$, and then $x^2 \equiv a \pmod{4}$ has two roots; and if $\kappa \geqq 3$ we must have $a \equiv 1 \pmod{8}$, and then $x^2 \equiv a \pmod{2^\kappa}$ has four incongruent roots.

If then t denote the number of different odd primes which divide m, the number of distinct solutions of the given congruence, when it is soluble, is

$$2^t,\ 2^{t+1},\ 2^{t+2}$$

according as $\kappa < 2$, $\kappa = 2$, $\kappa > 2$ respectively.

36. In order to complete the theory of quadratic congruences, two problems have still to be solved. They are, first, to determine practically whether the congruence $x^2 \equiv a \pmod{p}$ is possible, p being an odd prime, or, in other words, to find the value of $(a \mid p)$: and secondly to find the roots of the congruence when it has been shewn to be possible.

It follows from Art. 31 that the determination of $(a|p)$ may be made to depend upon that of the symbols $(-1|p)$, $(2|p)$, and $(q|p)$, where q is a positive odd prime. These three cases will now be considered in order.

37. By Art. 30, $(-1|p)=(-1)^{\frac{p-1}{2}}$: this is $+1$ if $\frac{1}{2}(p-1)$ is even. Putting $\frac{1}{2}(p-1)=2n$, this gives $p=4n+1$. On the other hand if p is of the form $4n+3$, $\frac{1}{2}(p-1)=2n+1$, and

$$(-1|p)=(-1)^{2n+1}=-1.$$

Hence -1 is a quadratic residue or non-residue of p according as p is of the form $4n+1$ or $4n+3$.

38. It is found by trial that 2 is a quadratic residue of 7, 17, 23, 31, 41, 47 and a non-residue of 3, 5, 11, 13, 19, 29, 37, 43. The first set are all of the form $8n \pm 1$, and the second set are all of the form $8n \pm 3$. It may be shewn that this law is general: namely that 2 is a residue of all primes of the form $8n \pm 1$ and a non-residue of all primes of the form $8n \pm 3$.

We begin with the latter part of the proposition, viz. that 2 is a non-residue of all primes of the form $8n \pm 3$. If this is not true, let p be the least prime of this form for which the congruence $x^2 \equiv 2 \pmod{p}$ is possible. Suppose $x=e$ is a solution of the congruence: then we may take e to be positive, less than p, and *odd*: for if the congruence is possible there are two suitable values of x which are positive and less than p, and their sum $=p$ which is odd, so that one of the values of x must be odd. Hence $e^2 \equiv 1 \pmod{8}$, and $e^2=2+pf$ where f is positive and less than p. Now $pf=e^2-2=-1 \pmod{8}$: and since $p=\pm 3 \pmod{8}$, $f \equiv \mp 3 \pmod{8}$. Consequently f must have at least one prime divisor q of the form $8n \pm 3$: for if all the factors were of the form $8n \pm 1$, their product would also be of this form. Since $f<p$ it follows that $q<p$: and evidently $e^2 \equiv 2 \pmod{f} \equiv 2 \pmod{q}$, so that p is not the smallest prime of the form $8n \pm 3$ of which 2 is a residue. This contradicts the hypothesis, and the second part of the proposition is therefore proved.

Next let p be of the form $8n+7$; then by Art. 37, -1 is a non-residue of p: hence to shew that $2Rp$, it is enough to prove that $-2Np$. Now it can be shewn that -2 is a non-residue of all primes of the form $8n+5$ or $8n+7$. For this is true when $p=5$ or 7, as we see by trial: and supposing p the least prime of either of these forms for which $x^2+2 \equiv 0 \pmod{p}$ is soluble, we may put as before $x = e$, and $e^2 + 2 = pf$, where e is positive, less than p, and odd. Hence $pf \equiv 3 \pmod{8}$, and therefore $f \equiv 7$ or $5 \pmod{8}$ according as $p \equiv 5$ or $7 \pmod{8}$. As in the other case we conclude that f must have at least one prime divisor q which is less than p and of the form $8n + 5$ or $8n + 7$: this gives $e^2 + 2 \equiv 0 \pmod{q}$, which contradicts the hypothesis: and therefore -2 is a non-residue of all primes of the form $8n + 5$ or $8n + 7$, as stated.

Finally suppose $p = 8n + 1$: then the preceding method is inapplicable. In this case, however, if g is a primitive root of p,

$$g^{4n} \equiv -1,$$

whence

$$(g^{2n} \pm 1)^2 \equiv \pm 2g^{2n};$$

and since

$$g^{8n} \equiv 1,$$

this gives

$$\pm 2 \equiv (g^n \pm g^{7n})^2.$$

This shews not only that $\pm 2Rp$, but also how the roots of $x^2 \equiv \pm 2$ may be found.

The different cases discussed in this article are all included in the formula

$$(2|p) = (-1)^{\frac{p^2-1}{8}}.$$

Legendre's Law of Reciprocity.

39. The practical determination of $(q|p)$, where q, p are positive odd primes, is effected by the help of a very important theorem, which is known as Legendre's Law of Reciprocity.

The theorem is that $(q|p) = (p|q)$, except when p and q are both of the form $4n + 3$, in which case $(q|p) = -(p|q)$. Both these results are included in the formula

$$(q|p)(p|q) = (-1)^{\frac{1}{4}(p-1)(q-1)}.$$

The first rigorous proof of this proposition was given by Gauss, who succeeded in discovering eight different demonstrations of it.

The following is essentially Gauss's third proof, as modified by Dirichlet[1].

For convenience write $p = 2p' + 1$, $q = 2q' + 1$. Consider the series of numbers

$$q, 2q, 3q, \ldots p'q:$$

[1] **Gauss: Theorematis arithmetici demonstratio nova (*Comm. Gott.* vol. 15, 1808, or *Werke*, II. p. 1). Dirichlet, *Zahlentheorie*, p. 99 (3rd edition).**

these are all incongruent (mod p): hence their least positive residues will be all incongruent (mod p). Of these least residues a certain number, μ suppose, will be greater than p': suppose these are $\alpha_1, \alpha_2, \dots \alpha_\mu$; and let the others, which are not greater than p', be denoted by $\beta_1, \beta_2 \dots \beta_\lambda$, so that $\lambda + \mu = p'$. Now the numbers

$$p - \alpha_1,\ p - \alpha_2, \dots p - \alpha_\mu$$

are all less than $p' + 1$, and all incongruent (mod p) since $\alpha_1, \alpha_2 \dots$ are so. Moreover none of the last series can be congruent to any one of the series $\beta_1, \beta_2 \dots \beta_\lambda$: for if we had $p - \alpha \equiv \beta$ (mod p) it would follow that $\alpha + \beta = p$, and consequently if α is a residue of sq, and β of tq, $sq + tq \equiv 0$ (mod p), and hence, since q is prime, $s + t \equiv 0$ (mod p), which is impossible, since s and t are both less than $\frac{1}{2}p$. Consequently the series

$$(p - \alpha_1),\ (p - \alpha_2) \dots (p - \alpha_\mu),\ \beta_1, \beta_2 \dots \beta_\lambda$$

must consist of the numbers 1, 2, 3 ... p' only in a different order; and therefore

$$\begin{aligned} 1 \,.\, 2 \,.\, 3 \dots p' &\equiv (p - \alpha_1)(p - \alpha_2) \dots (p - \alpha_\mu) \,.\, \beta_1 \beta_2 \dots \beta_\lambda \pmod{p} \\ &\equiv (-1)^\mu \,.\, \alpha_1 \alpha_2 \dots \alpha_\mu \,.\, \beta_1 \beta_2 \dots \beta_\lambda \pmod{p}. \end{aligned}$$

But
$$\begin{aligned} \alpha_1 \alpha_2 \dots \alpha_\mu \,.\, \beta_1 \beta_2 \dots \beta_\lambda &\equiv q \,.\, 2q \,.\, 3q \dots p'q \\ &\equiv q^{p'} \,.\, 1 \,.\, 2 \,.\, 3 \dots p' \end{aligned}$$

and therefore

$$(-1)^\mu \,.\, q^{p'} \,.\, 1 \,.\, 2 \,.\, 3 \dots p' \equiv 1 \,.\, 2 \,.\, 3 \dots p' \pmod{p}.$$

Dividing by $1 \,.\, 2 \,.\, 3 \dots p'$ which is prime to p, we get

$$(-1)^\mu \,.\, q^{p'} \equiv 1 \pmod{p}$$

or
$$q^{p'} \equiv (-1)^\mu \pmod{p}.$$

But
$$q^{p'} \equiv (q \mid p) \pmod{p} \text{ by Art. 30}:$$

therefore finally $(q \mid p) = (-1)^\mu$. It remains to calculate the value of this expression.

It is convenient in what follows to denote by $[x]$ the greatest positive integer contained in the real positive quantity x; so that $x = [x] + \theta$ where θ is a positive proper fraction. Making use of this notation we may write

$$\begin{aligned} q &= p\,[q/p] + r_1 \\ 2q &= p\,[2q/p] + r_2 \\ \vdots\ \ & \quad\ \ \vdots \qquad\ \ \vdots \\ p'q &= p\,[p'q/p] + r_{p'}, \end{aligned}$$

where $r_1, r_2 \dots r_{p'}$ are all positive and less than p: hence by addition

$$\frac{p^2-1}{8} \cdot q = Mp + A + B \qquad (1),$$

where

$$M = [q/p] + [2q/p] + \dots + [p'q/p]$$

$$A = \alpha_1 + \alpha_2 + \dots + \alpha_\mu$$

$$B = \beta_1 + \beta_2 + \dots + \beta_\lambda.$$

Now

$$(p-\alpha_1) + (p-\alpha_2) + \dots + (p-\alpha_\mu) + \beta_1 + \beta_2 + \dots + \beta_\lambda = 1 + 2 + 3 + \dots + p',$$

that is

$$\mu p - A + B = \frac{p^2-1}{8}.$$

Combining this with (1) we have

$$\frac{p^2-1}{8}(q-1) = (M-\mu)p + 2A.$$

Now $\frac{p^2-1}{8}$ is an integer, since p is odd; also $(q-1)$ is even: therefore $(M-\mu)p \equiv 0 \pmod 2$ and hence $\mu = M \pmod 2$, so that $(q|p) = (-1)^\mu = (-1)^M$.

In exactly the same way

$$(p|q) = (-1)^N$$

where

$$N = [p/q] + [2p/q] + \dots + [q'p/q].$$

Of the two numbers p, q one must be less than the other: suppose $q < p$.

Then in the expression M no term $[(s+1)q/p]$ can exceed the preceding term by more than 1, because $\frac{(s+1)q}{p} - \frac{sq}{p} = \frac{q}{p}$ which is a proper fraction: moreover if $[(s+1)q/p] = [sq/p] + 1$ there will be a positive integer t such that

$$\frac{sq}{p} < t < \frac{(s+1)q}{p}:$$

from which

$$s < \frac{tp}{q} < s+1$$

so that $s = [tp/q]$. In other words, $[sq/p] = t - 1$ when s has any one of the values

$$[(t-1)p/q]+1,\ [(t-1)p/q]+2, \dots [tp/q];$$

$\{[tp/q] - [(t-1)p/q]\}$ values in all.

Hence the expression for M becomes

$$\begin{aligned}0\,.\,[p/q] + 1\,.\,\{[2p/q]-[p/q]\} + 2\,.\,\{[3p/q]-[2p/q]\} + \dots\\ + (q'-1)\,.\,\{[q'p/q]-[(q'-1)\,p/q]\}\\ + q'\,.\,\{p'-[q'p/q]\}.\end{aligned}$$

the last term being obtained by observing that there are p' terms in the original expression for M.

Rearranging, we get

$$\begin{aligned}M &= p'q' - \{[p/q]+[2p/q]+[3p/q]+\dots+[q'p/q]\}\\ &= p'q' - N,\end{aligned}$$

or

$$M+N=p'q'.$$

Therefore finally

$$\begin{aligned}(q\,|\,p)\,(p\,|\,q) &= (-1)^{M+N} = (-1)^{p'q'}\\ &= (-1)^{\frac{1}{4}(p-1)(q-1)}.\end{aligned}$$

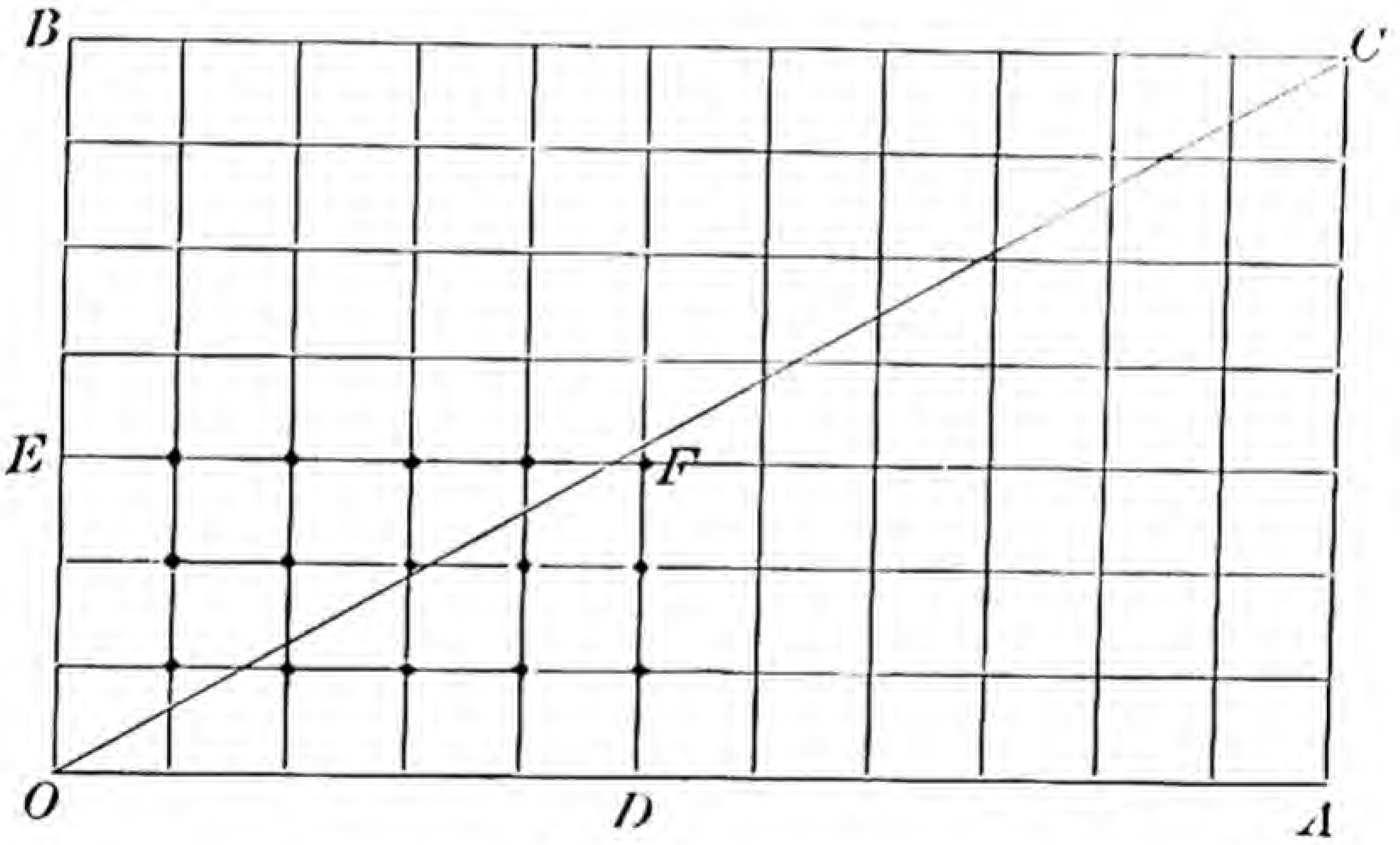

Fig. 1.

40. Eisenstein[1] has put into a simple geometrical form that part of the preceding demonstration which consists in shewing that $M+N=p'q'$.

Construct a rectangle $OACB$ of which the sides OA, OB contain p and q units of length respectively: divide this up into unit squares as in the figure. Join OC: and let $OD=EF=p'$ $OE=DF=q'$.

Take OA for axis of x, OB for axis of y, and for shortness' sake let a point (a, b) where a, b are positive integers (neither zero) be called a node.

[1] Crelle, vol. 27, p. 322.

The equation of OC is $y = \frac{q}{p}x$: since q/p is in its lowest terms there are no nodes on the diagonal OC.

Evidently $[mq/p]$ is the number of nodes contained in that part of the line $x = m$ which is intercepted between OA and OC.

Hence $M = [q/p] + [2q/p] + \dots + [p'q/p]$ is the number of nodes included between the lines OC, OD, DF, those upon DF being counted in.

Similarly N is the number of nodes included between OC, OE, EF.

Therefore $M + N$ is the number of nodes belonging to the rectangle $ODFE$, that is, $M + N = p'q'$.

41. As an example of the practical use of the Law of Reciprocity, suppose it is required to find whether the congruence

$$x^2 + 1457 \equiv 0 \pmod{2389}$$

is possible.

Here 2389 is a prime: and

$$(-1457\,|\,2389) = (-1\,|\,2389)(31\,|\,2389)(47\,|\,2389).$$

Now $(-1\,|\,2389) = +1$, since $2389 \equiv 1 \pmod 4$:

$$(31\,|\,2389) = (2389\,|\,31) = (2\,|\,31), \text{ [since } 2389 \equiv 2 \pmod{31}]$$
$$= +1 \text{ by Art. 38};$$

$$(47\,|\,2389) = (2389\,|\,47) = (39\,|\,47) = (3\,|\,47)(13\,|\,47)$$
$$= -(47\,|\,3)(47\,|\,13) = -(2\,|\,3)(8\,|\,13)$$
$$= -(2\,|\,3)(2\,|\,13) = -(-1)(-1) = -1$$

[or, more simply, $(39\,|\,47) = (-8\,|\,47) = (-2\,|\,47) = -1$].

Finally, therefore, $(-1457\,|\,2389) = (+1)(+1)(-1)$
$$= -1;$$

so that the proposed congruence is insoluble.

42. The meaning of Legendre's symbol $(q\,|\,p)$ has been extended by Jacobi[1] as follows.

Let the positive odd number P be resolved into its prime factors $p, p', p'' \dots$ so that

$$P = pp'p'' \dots$$

[1] *Berlin Monatsberichte*, 1837: or Crelle, vol. 30, p. 166.

and let m be any integer prime to P. Then the symbol $(m|P)$ is defined by the equation

$$(m|P)=(m|p)(m|p')(m|p'')\ldots\ldots$$

where, of course, two or more of the primes $p, p', p''\ldots$ may be identical.

Observe that when P is an odd prime, the meaning of Jacobi's symbol coincides with that of Legendre's; and that when P is even, the symbol $(m|P)$ does not exist.

The properties of the generalised symbol are expressed by the following theorems.

1. If m is prime to each of the odd numbers P, Q,

$$(m|PQ)=(m|P)(m|Q).$$

For if
$$P=pp'p''\ldots$$
$$Q=qq'q''\ldots$$
$$(m|PQ)=(m|p)(m|p')(m|p'')\ldots(m|q)(m|q')(m|q'')\ldots$$
$$=(m|P)(m|Q).$$

2. If $l, m, n\ldots$ are all prime to P, then

$$(lmn\ldots|P)=(l|P)(m|P)(n|P)\ldots.$$

For if
$$P=pp'p''\ldots \text{ as before,}$$
$$(l|P)=(l|p)(l|p')(l|p'')\ldots$$
$$(m|P)=(m|p)(m|p')(m|p'')\ldots$$
$$(n|P)=(n|p)(n|p')(n|p'')\ldots \text{ etc.}$$

Now by Art. 31, $(l|p)(m|p)(n|p)\ldots=(lmn\ldots|p)$: so that, multiplying the preceding equations together, we get

$$(l|P)(m|P)(n|P)\ldots=(lmn\ldots|p)(lmn\ldots|p')(lmn\ldots|p'')$$
$$=(lmn\ldots|P).$$

3. If $m'\equiv m \pmod{P}$ and m is prime to P, then m' is also prime to P, and $(m'|P)=(m|P)$.

This is obvious, since $m'\equiv m \pmod{p}$ and therefore

$$(m'|p)=(m|p):$$

and so for any other prime factor of P.

Before discussing the symbols $(-1|P)$ and $(2|P)$, the following two lemmas are necessary.

I. If $R = rr'r''\dots$ is any odd number

$$\frac{R-1}{2} \equiv \frac{r-1}{2} + \frac{r'-1}{2} + \dots \equiv \Sigma \frac{r-1}{2} \pmod{2}.$$

II. With the same notation

$$\frac{R^2-1}{8} \equiv \Sigma \frac{r^2-1}{8} \pmod{2}.$$

The proof is very simple: namely

$$R = (1 + \overline{r-1})(1 + \overline{r'-1})(1 + \overline{r''-1})\dots$$
$$\equiv 1 + \Sigma(r-1) \pmod{4},$$

and therefore
$$\frac{R-1}{2} = \Sigma \frac{r-1}{2} \pmod{2}.$$

Similarly
$$R^2 = (1 + \overline{r^2-1})(1 + \overline{r'^2-1})\dots$$
$$= 1 + \Sigma(r^2-1) \pmod{16},$$

therefore
$$\frac{R^2-1}{8} = \Sigma \frac{r^2-1}{8} \pmod{2}.$$

4. P, as before, being an odd positive number,

$$(-1|P) = (-1)^{\frac{P-1}{2}},$$
$$(2|P) = (-1)^{\frac{P^2-1}{8}}.$$

For by definition

$$(-1|P) = (-1|p)(-1|p')(-1|p'')\dots$$
$$= (-1)^{\frac{p-1}{2}}(-1)^{\frac{p'-1}{2}}\dots$$
$$= (-1)^{\Sigma\frac{p-1}{2}} = (-1)^{\frac{P-1}{2}} \text{ by Lemma I.}$$

and similarly
$$(2|P) = (-1)^{\Sigma\frac{p^2-1}{8}} = (-1)^{\frac{P^2-1}{8}}$$
by Lemma II.

5. If the positive odd numbers P, Q are prime to each other,

$$(P|Q)(Q|P) = (-1)^{\frac{1}{4}(P-1)(Q-1)}.$$

Namely, if $P = pp'p''\dots$ and $Q = qq'q''\dots$ it follows from theorems (1) and (2) that

$$(P|Q) = \Pi\,(p|q),$$

where the product extends over all the different combinations of a factor p with a factor q.

Similarly $(Q|P) = \Pi\,(q|p)$, and therefore

$$\begin{aligned}(P|Q)(Q|P) &= \Pi\,(p|q)(q|p)\\ &= \Pi\,(-1)^{\frac{1}{4}(p-1)(q-1)}\\ &= (-1)^{\Sigma\frac{1}{4}(p-1)(q-1)}.\end{aligned}$$

Now since the summation extends over every combination (p, q)

$$\begin{aligned}\Sigma\,\tfrac{1}{4}(p-1)(q-1) &= \Sigma\frac{p-1}{2} \times \Sigma\frac{q-1}{2}\\ &\equiv \frac{P-1}{2}\cdot\frac{Q-1}{2}\ (\text{mod } 2),\end{aligned}$$

by Lemma I.

Hence $(P|Q)(Q\ P) = (-1)^{\frac{P-1}{2}\,\frac{Q-1}{2}} = (-1)^{\frac{1}{4}(P-1)(Q-1)}$.

It is clear that by means of Jacobi's extension of the law of reciprocity the algorithm for finding $(q|p)$ may often be abbreviated. For instance, in the latter part of the example of Art. 41 we may proceed thus:

$$(39|47) = -(47|39) = -(8|39) = -(2|39) = -1:$$

the resolution of 39 into its prime factors being avoided.

43. Like many other important theorems, the law of quadratic reciprocity was first proved by an inductive method. Gauss's original proof (*D. A.* Arts. 125—144) has been considerably simplified, without altering its character, by Dirichlet (Crelle, t. 47, p. 139). As it is an admirable example of mathematical induction, it seems proper to reproduce it here.

It is assumed that the formula

$$(p|q)(q|p) = (-1)^{\frac{1}{4}(p-1)(q-1)},$$

where p and q are positive odd primes, has been proved for all such primes which are less than a particular prime, say q: it is then shewn to be true for every combination of q with a smaller prime: the theorem being true in the case of the two smallest primes 3, 5 it is thus seen to be true universally.

We observe in the first place that if Legendre's formula is true for every combination of two primes less than q, Jacobi's generalised formula $(P|Q)(Q|P) = (-1)^{\frac{1}{4}(P-1)(Q-1)}$ is also true, provided P, Q are positive odd numbers, every prime divisor of which is less than q. This is obvious from Art. 42.

It will further be supposed that the results of Arts. 37, 38 with respect to the values of $(-1|p)$ and $(\pm 2|p)$ have been proved: from these follow the values of the generalised symbols $(-1|P)$, and $(\pm 2|P)$ by Art. 42.

The complete proof requires the discussion of three separate cases.

I. First let pRq: then an integer e can be found such that

$$e^2 - p = qf.$$

Further, we may suppose e less than q and *even*: for there are two suitable values of e which are less than q, and their sum is q which is odd: hence one of the values of e must be even. Hence f is odd, positive, and less than q.

Now if f is not divisible by p, it follows from the above equation that $(p|f) = 1$, and $(qf|p) = 1$, that is, $(q|p)(f|p) = 1$.

Hence by multiplication,

$$(q|p)(f|p)(p|f) = 1,$$

or
$$(q|p) = (f|p)(p|f) = (-1)^{\frac{1}{4}(p-1)(f-1)}$$

by the extended law of reciprocity. Now by Lemma I. of Art. 42

$$\frac{q-1}{2} + \frac{f-1}{2} \equiv \frac{qf-1}{2} \pmod 2$$

$$\equiv \frac{e^2-(p+1)}{2} \pmod 2$$

$$\equiv -\frac{p+1}{2} \pmod 2 \text{ since } e \text{ is even,}$$

$$\therefore \quad \frac{p-1}{2} \cdot \frac{q-1}{2} + \frac{p-1}{2} \cdot \frac{f-1}{2} \equiv -\frac{p^2-1}{4} \pmod 2$$

$$\equiv 0 \pmod 2,$$

$$\therefore \quad (q|p) = (-1)^{\frac{1}{4}(p-1)(f-1)} = (-1)^{\frac{1}{4}(p-1)(q-1)}$$

which agrees with the law of reciprocity, since $(p|q) = 1$.

If f is divisible by p, so also is e, and we may write $e = e'p$, $f = f'p$, so that

$$e'^2p - 1 = qf'$$

where e' is even, and f' is odd and less than q.

Hence $e'^2p \equiv 1 \pmod{f'}$ and therefore $(p|f') = 1$.

Also
$$(-qf'|p) = 1:$$

that is,
$$(-1)^{\frac{p-1}{2}}(q|p)(f'|p) = 1:$$

multiplying, etc. as in the other case, we infer that

$$(q|p) = (-1)^{\frac{p-1}{2} + \frac{1}{4}(p-1)(f'-1)}$$
$$= (-1)^{\frac{1}{4}(p-1)(f'+1)}.$$

Since $qf' \equiv -1 \pmod 4$, one of the numbers q, f' must be of the form $4n + 1$ and the other of the form $4n + 3$, whence

$$\frac{f'+1}{2} \equiv \frac{q-1}{2} \pmod 2:$$

and therefore

$$(q|p) = (-1)^{\frac{1}{4}(p-1)(q-1)}$$

as before.

II. Next suppose pNq and $q \equiv 3 \pmod 4$: then $-pRq$, and we may write

$$e^2 + p = qf$$

where, as before, e is even, and f odd, and less than q.

Hence $$1 = (-p|f) = (-1)^{\frac{f-1}{2}}(p|f)$$

and $$1 = (qf|p) = (q|p)(f|p):$$

therefore $$(q|p) = (-1)^{\frac{f-1}{2}}(p|f)(f|p)$$
$$= (-1)^{\frac{1}{4}(p+1)(f-1)}.$$

Now since $qf \equiv p \pmod 4$ and $q \equiv 3 \pmod 4$, $f \equiv 1$ or $3 \pmod 4$ according as $p \equiv 3$ or $1 \pmod 4$: therefore $p - f \equiv 2 \pmod 4$, and consequently

$$\tfrac{1}{4}(p+1)(f-1) - \tfrac{1}{4}(p-1)(f+1) = \tfrac{1}{2}(f-p) \equiv 1 \pmod 2$$

therefore $$(q|p) = -(-1)^{\frac{1}{4}(p-1)(f+1)}.$$

As in Lemma I.

$$(q-1) + (f+1) \equiv qf + 1 \pmod 4$$
$$= p + 1 \pmod 4;$$

$$\therefore \quad (p-1)(q-1) + (p-1)(f+1) \equiv p^2 - 1 \pmod 8,$$
$$\equiv 0 \pmod 8,$$

$$\therefore \quad \tfrac{1}{4}(p-1)(q-1) + \tfrac{1}{4}(p-1)(f+1) \equiv 0 \pmod 2,$$

and therefore finally $(q|p) = -(-1)^{\frac{1}{4}(p-1)(q-1)}$ which agrees with the law of reciprocity, since $(p|q) = -1$.

If p divides f, we put, as before, $e = e'p$, $f = f'p$,

$$e'^2p + 1 = qf',$$

where f' is odd and $\equiv 3 \pmod 4$.

Hence $$(p|f') = -1$$

$$1 = (qf'|p) = (q|p)(f'|p)$$

and $$(q|p) = -(p|f')(f'|p) = -(-1)^{\frac{1}{4}(p-1)(f'-1)}$$
$$= -(-1)^{\frac{1}{4}(p-1)(q-1)}$$

since $$f' \equiv q \pmod{4}.$$

44. The case which remains to be discussed is that in which pNq and $q \equiv 1 \pmod{4}$. It has to be shewn that in this case qNp. The proof is effected with the help of the following lemma:—

There exists a prime number p' less than q such that qNp'.

When $q \equiv 5 \pmod{8}$, this is easily proved: namely $q - 2 \equiv 3 \pmod{8}$, and therefore $q - 2$ involves at least one prime factor of the form $8n + 3$ or $8n + 5$: if p' be any such factor, $q - 2 \equiv 0 \pmod{p'}$, and therefore

$$(q|p') = (2|p') = -1.$$

Next suppose $q \equiv 1 \pmod{8}$.

Let m be the greatest integer which is less than $\sqrt{q}$, and suppose, if possible, that q is a quadratic residue of all odd primes which do not exceed $2m + 1$. Then if $M = (2m + 1)!$ the congruence $x^2 \equiv q \pmod{M}$ is possible (cf. Art. 35), and we may therefore find a positive integer k such that $k^2 \equiv q \pmod{M}$.

Hence

$$(q - 1^2)(q - 2^2)\ldots(q - m^2) \equiv (k^2 - 1^2)(k^2 - 2^2)\ldots(k^2 - m^2) \pmod{M}.$$

Now $$k(k^2 - 1^2)(k^2 - 2^2)\ldots(k^2 - m^2)$$
$$= (k + m)(k + m - 1)(k + m - 2)\ldots k(k - 1)\ldots(k - m),$$

and since this is the product of $(2m + 1)$ consecutive integers it is divisible by $(2m + 1)!$ i.e. by M, so that

$$k(q - 1^2)(q - 2^2)\ldots(q - m^2) \equiv 0 \pmod{M},$$

and therefore, since k is prime to M,

$$(q - 1^2)(q - 2^2)\ldots(q - m^2)/M$$

is an integer.

But this quotient may be written in the form

$$\frac{1}{m+1} \cdot \frac{q - 1^2}{(m+1)^2 - 1^2} \cdot \frac{q - 2^2}{(m+1)^2 - 2^2} \cdots \frac{q - m^2}{(m+1)^2 - m^2},$$

where each factor is a proper fraction: so that it cannot be an integer.

Thus there must be at least one prime less than $2m+1$, of which q is a non-residue: and $2m+1 < 2\sqrt{q}+1 < q$, since q is at least equal to 17. The lemma is therefore proved.

45. We are now able to complete the proof of the law of reciprocity.

Observe in the first place that with the notation of last article $p'Nq$, for if p' were a residue of q, it would follow by Art. 43 that qRp', which is not true. Since then pNq and $p'Nq$, it follows that $pp'Rq$, and we may write

$$e^2 - pp' = qf,$$

where e is even and less than q, and f consequently odd and less than q.

I. Suppose neither p nor p' divides f.

Then $\quad (pp'|f)=1, \quad (qf|pp')=(q|pp')(f|pp')=1:$

$\therefore$ by multiplication

$$(q|pp')(f|pp')(pp'|f)=1,$$

or
$$(q|pp')=(f|pp')(pp'|f)=(-1)^{\frac{1}{4}(pp'-1)(f-1)}.$$

Now since $q \equiv 1 \pmod 4$ and e is even,

$$pp' \equiv -f \pmod 4,$$

and therefore one of the numbers $\dfrac{pp'-1}{2}$, $\dfrac{f-1}{2}$ is even, so that $(q|pp')=+1$, and therefore since $(q|p')=-1$,

$$(q|p)=-1.$$

II. Next suppose f divisible by p' but not by p. Put $f=f'p'$, $e=e'p'$; then

$$e'^2p'-p=qf',$$

where f' is odd and prime to p and p', and e' is even.

Hence $\quad pp' \equiv e'^2p'^2 \pmod{f'}$,

so that $\quad (pp'|f')=1:$

and similarly $\quad (p'qf'|p)=1, \quad (-pqf'|p')=1,$

$\therefore$ by multiplication

$$(q|pp')(pp'|f')(f'|pp')(p'|p)(-p|p')=1,$$

or
$$(q|pp')=(-1)^{\frac{1}{4}(pp'-1)(f'-1)}.(-1)^{\frac{1}{4}(p-1)(p'-1)}.(-1)^{\frac{1}{2}(p'-1)}$$
$$=(-1)^{\frac{1}{4}(pp'-1)(f'-1)+\frac{1}{4}(p+1)(p'-1)}=(-1)^{\lambda} \text{ say.}$$

Now since $$f' \equiv -p \pmod{4},$$

$$\frac{f'-1}{2} \equiv \frac{p+1}{2} \pmod{2}:$$

also $$\tfrac{1}{2}(pp'-1) = \tfrac{1}{2}(p-1) + \tfrac{1}{2}(p'-1) \pmod{2}:$$

so that the index λ is congruent (mod 2) to

$$\left(\frac{p-1}{2} + \frac{p'-1}{2}\right)\left(\frac{p+1}{2}\right) + \tfrac{1}{4}(p+1)(p'-1),$$

that is to $$\tfrac{1}{4}(p^2-1) + \tfrac{1}{2}(p+1)(p'-1),$$

which is evidently even. Hence

$$(q \mid pp') = +1,$$

and therefore as before $$(q \mid p) = -1.$$

The case in which f is divisible by p but not by p' may be similarly treated.

III. Finally suppose f is divisible by pp'.

Putting $$e = e'pp', \quad f = f'pp',$$

we get $$e'^2pp' - 1 = qf',$$

whence $$(pp' \mid f') = 1,$$

$$(-qf' \mid pp') = (q \mid pp')(-f' \mid pp') = 1,$$

and therefore $$\begin{aligned}(q \mid pp') &= (-f' \mid pp')(pp' \mid f') \\ &= (-1)^{\frac{1}{4}(pp'-1)(f'+1)}.\end{aligned}$$

Now $f' \equiv -1 \pmod{4}$ so that $\dfrac{f'+1}{2}$ is even, and therefore $(q \mid pp') = +1$, and thence as before $(q \mid p) = -1$.

The law of reciprocity has therefore been completely proved.

46. It is now easy to find the forms of the prime numbers of which a given number D is a quadratic residue: more generally, we can determine all the positive numbers n which are prime to $2D$, and such that $(D \mid n) = +1$[1].

Evidently we may suppose that D is not divisible by any square: for if $D = a^2D'$,

$$(D \mid n) = (a^2 \mid n)(D' \mid n) = (D' \mid n).$$

If then P denotes the positive product of all the odd primes which divide D, we have

$$D = \pm P, \text{ or } D = \pm 2P.$$

[1] Cf. Dirichlet, *Zahlentheorie*, p. 121.

There are four cases to consider:

I. $$D = \pm P \equiv 1 \pmod{4}.$$

By the generalised law of reciprocity

$$(D|n) = (n|P).$$

Now $$(n'|P) = (n|P) \text{ if } n' \equiv n \pmod{P}:$$

moreover n is to be odd: so that it is sufficient to consider the $\phi(P)$ odd numbers which are less than $2P$ and prime to P.

Let a be any one of these numbers for which $(a|P) = +1$: then $(D|n) = +1$, and n is odd, if

$$n \equiv a \pmod{2P}.$$

Similarly $(D|n) = -1$, and n is odd, if

$$n \equiv b \pmod{2P},$$

where b is any one of the numbers less than $2P$ and prime to it, for which $(b|P) = -1$.

For instance if $D = 13$, the odd residues of 13 which are less than 26 are

$$1,\ 3,\ 9,\ 17,\ 23,\ 25:$$

so that $(13|n) = 1$ if $n \equiv 1, 3, 9, 17, 23, 25 \pmod{26}$,

and $(13|n) = -1$ if $n = 5, 7, 11, 15, 19, 21 \pmod{26}$.

II. $$D = \pm P \equiv 3 \pmod{4}.$$

Here $$(D|n) = (-1)^{\frac{n-1}{2}} (n|P),$$

so that $$(D|n) = +1$$

if $$(n|P) = +1, \quad n \equiv 1 \pmod{4},$$
$$\textit{or } (n|P) = -1, \quad n \equiv 3 \pmod{4}:$$

while $(D|n) = -1$ if

$$(n|P) = +1, \quad n \equiv 3 \pmod{4},$$
$$\textit{or } (n|P) = -1, \quad n \equiv 1 \pmod{4}.$$

III. $$D = \pm 2P \equiv 2 \pmod{8}.$$

In this case $$(D|n) = (-1)^{\frac{1}{8}(n^2-1)} . (n|P):$$

$$(D|n) = +1 \text{ if } (n|P) = +1, \quad n \equiv \pm 1 \pmod{8}$$
$$\textit{or } (n|P) = -1, \quad n \equiv \pm 3 \pmod{8},$$
$$(D|n) = -1 \text{ if } (n|P) = -1, \quad n \equiv \pm 1 \pmod{8}$$
$$\textit{or } (n|P) = +1, \quad n \equiv \pm 3 \pmod{8}.$$

IV. $$D = \pm 2P \equiv 6 \pmod 8.$$

$$(D|n) = (-1)^{\frac{1}{2}(n-1)+\frac{1}{8}(n^2-1)} \cdot (n|P)$$

$$\begin{array}{lll} (D|n) = +1 & \text{if } (n|P) = +1 & n \equiv 1, 3 \pmod 8 \\ & \text{or } (n|P) = -1 & n \equiv 5, 7 \pmod 8 \\ (D|n) = -1 & \text{if } (n|P) = -1 & n \equiv 1, 3 \pmod 8 \\ & \text{or } (n|P) = +1 & n \equiv 5, 7 \pmod 8). \end{array}$$

In each of the cases II--IV the values of n group themselves into arithmetical progressions with a common difference $4D$ instead of $2D$ as in the first case.

Example. Let $D = -30$: this is a case of III, with $P = 15$. It will be found that $(n|15) = +1$ if $n \equiv 1, 2, 4, 8 \pmod{15}$ and that $(n|15) = -1$ if $n \equiv 7, 11, 13, 14 \pmod{15}$.

The conditions $(n|15) = +1$, $n \equiv \pm 1 \pmod 8$ are simultaneously satisfied if

$$n \equiv 1, 17, 23, 31, 47, 49, 79, 113 \pmod{120};$$

and $(n|15) = -1$, $n \equiv \pm 3 \pmod 8$ simultaneously if

$$n \equiv 11, 13, 29, 37, 43, 59, 67, 101 \pmod{120}.$$

Thus $(-30|n) = +1$ if

$$n \equiv 1, 11, 13, 17, 23, 29, 31, 37, 43, 47, 49, 59, 67, 79, 101, 113 \pmod{120}.$$

It should be carefully remembered that if n is a composite odd number the condition $(D|n) = +1$ is necessary but not sufficient in order that D may be a quadratic residue of n. The necessary and sufficient conditions are that $(D|p) = +1$ for every odd prime p which is contained in n (cf. Arts. 33—35). For instance

$$(2|15) = +1,$$

because $$(2|15) = (2|3)(2|5) = (-1)(-1) = +1;$$

but 2 is not a residue of 15.

The integers of which a given number D is a quadratic residue are sometimes referred to as the divisors of the form $x^2 - D$, or of the form $x^2 - Dy^2$: the meaning of the expression being that integral values of x and y, prime to each other, can be found so as to make $x^2 - Dy^2$ a multiple of the divisor in question. Thus the problem of the present article has been completely discussed by Legendre under the head of "finding the linear forms which belong to the divisors of $t^2 \pm cu^2$" (*Théorie des Nombres,* 2ième Partie,

§§ X—XII): and he gives at the end of his work (Tables III—VII) lists of the odd linear divisors of a large number of forms $t^2 \pm cu^2$. A comparison of Legendre's method with that here given will shew that both agree in principle, but that a good deal of clearness and brevity is gained by the use of the extended law of reciprocity.

47. The practical solution of the congruence $x^2 = a \pmod{p}$, when its possibility has been established, is by no means easy when p is a large prime. A direct solution may be given when p is of the form $4n+3$ or $8n+5$. Namely if $p = 4n+3$ and aRp

$$a^{2n+1} \equiv 1 \pmod{p};$$

whence

$$a \equiv a^{2n+2} \pmod{p},$$

and the roots of

$$x^2 \equiv a \pmod{p} \text{ are therefore}$$

$$x \equiv \pm a^{n+1} \pmod{p}.$$

Similarly when $p = 8n+5$ and aRp

$$a^{4n+2} - 1 \equiv 0 \pmod{p};$$

whence either

$$a^{2n+1} \equiv 1 \pmod{p}$$

or

$$a^{2n+1} \equiv -1 \pmod{p}.$$

In the former case $a^{2n+2} \equiv a$

and the solution is given by $x \equiv \pm a^{n+1}$.

In the latter case, since

$$\begin{aligned} -1 &\equiv (8n+4)! \text{ (by Wilson's Theorem)} \\ &\equiv 1^2 . 2^2 . 3^2 \ldots (4n+2)^2 \\ &\equiv M^2 \text{ (say)}, \\ a^{2n+1} &\equiv M^2. \end{aligned}$$

Now determine y so that $ay \equiv 1 \pmod{p}$: then multiplying the last congruence by y^{2n},

$$a \equiv y^{2n} M^2,$$

and therefore

$$x \equiv \pm My^n.$$

When $p \equiv 1 \pmod{8}$ an indirect method has generally to be adopted: and in fact, as Gauss has remarked, indirect methods are always preferable to the preceding, as being less laborious. Gauss has given a "method of exclusion," which may be applied with advantage when p is moderately large.

The solution of the congruence $x^2 \equiv a \pmod{p}$ is identical with that of the indeterminate equation

$$x^2 = py + a.$$

We may suppose that x is positive and less than $\frac{1}{2}p$: hence $x^2 < \frac{1}{4}p^2$ and the values of y which have to be considered range from 0 to $[\frac{1}{4}p]$, it being supposed that a is positive and less than p.

Now take any number e which is prime to p and greater than 2: find its non-residues n_1, n_2, n_3 etc. and denote the roots of the congruences

$$a + py \equiv n_1, \quad a + py \equiv n_2, \text{ etc. (mod } e)$$

by ν_1, ν_2, etc. Then if $y \equiv \nu_i$ (mod e), the expression $py + a$ is a non-residue of e and therefore cannot be a square. We are thus enabled to reject all the quantities $py + a$, where $y \equiv \nu_i$ (mod e); and by taking different numbers e, the series of integers $py + a$ which have to be tested may be continually reduced, until a sufficiently small number of them remain.

As an example take

$$x^2 \equiv 73 \text{ (mod } 127)$$

or

$$x^2 = 127y + 73.$$

Here y ranges from 1 to 31.

Taking $\quad e = 3, \quad n_1 = 2;$

and $\quad 73 + 127y \equiv 2 \text{ (mod } 3)$

gives $\quad y \equiv 1 \text{ (mod } 3).$

This leaves

2, 3, 5, 6, 8, 9, 11, 12, 14, 15, 17, 18
20, 21, 23, 24, 26, 27, 29, 30.

If $\quad e = 5, \quad n_1 = 2, \quad n_2 = 3;$

$$127y + 73 \equiv 2 \text{ (mod } 5)$$

gives $\quad 2y + 3 \equiv 2 \text{ (mod } 5), \quad \nu_1 = 2;$

$$127y + 73 \equiv 3 \text{ (mod } 5)$$

gives $\quad 2y + 3 \equiv 3 \text{ (mod } 5), \quad \nu_2 = 0.$

The series is now reduced to

3, 6, 8, 9, 11, 14, 17, 18, 21, 23, 24, 26, 29.

Next let $\quad e = 7$

$$n_1 = 3, \quad n_2 = 5, \quad n_3 = 6.$$

The congruences $\quad 127y + 73 \equiv 3, 5, 6 \text{ (mod } 7)$

or $\quad y + 3 \equiv 3, 5, 6 \text{ (mod } 7)$

give $\quad y \equiv 0, 2, 3 \text{ (mod } 7)$ respectively:

and the reduced series is now

$$6, 8, 11, 18, 26, 29:$$

we find by trial that

$$73 + 8 . 127 = 1089 = 33^2,$$

so that the solution of the given congruence is

$$x \equiv \pm 33 \pmod{127}.$$

Various considerations enable us to simplify the work of exclusion (cf. Gauss, *D. A.* Arts. 321, 322): in particular, if e, e' are relative primes, every number which is a residue of e and e' is a residue of ee', so that when two such "excluding numbers" e and e' have been used, there is no use in trying ee'. Again every residue of e is also a residue of $2e$, if e is odd: so that in this case $2e$ need not be tried, if e has been used.

AUTHORITIES.

Euler: *Observationes circa divisionem quadratorum per numeros primos* (Comm. Arith. i. p. 477). *Disquisitio accuratior circa residua ex divisione quadratorum altiorumque potestatum per numeros primos relicta* (ibid. i. p. 487). *Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia* (ibid. i. p. 516).

Legendre: *Recherches d'analyse indéterminée* (Hist. de l'Acad. Roy. des Sciences 1785, p. 465).

Gauss: *D. A.* Arts. 94—152.

Dirichlet-Dedekind: *Zahlentheorie*, §§ 32—52.

The literature connected with the quadratic law of reciprocity is very extensive. The reader who wishes to be fully acquainted with it should consult Baumgart (Osw.), *Ueber das quadratische Reciprocitätsgesetz* (Leipzig, 1885). Euler, by induction, discovered the law in its complete form (Comm. Arith. i. 486, 487; cf. Smith's *Report*, Art. 16, and Kronecker, *Zur Geschichte des Reciprocitätgesetzes*, Berl. Monatsber. 1875, p. 267) but did not prove it. Legendre, in the memoir above quoted, invented the symbol which goes by his name, stated the law in the form in which it is now generally given, and proved some cases of it; but the first complete demonstration was given by Gauss. It may be convenient to give here a complete list of Gauss's proofs of the *theorema fundamentale*, as he called it.

(i) *Disq. Arith.* Arts. 125—144. There are two curious MS. notes by Gauss to Art. 131: *Theorema fundamentale per inductionem detectum* 1795 *Martio*, and *Demonstratio prima, quæ in hac sectione traditur, inventa* 1796 *Apr.*, from which it would appear that he discovered the law of reciprocity independently of Euler and Legendre.

(ii) *Disq. Arith.* Art. 262. (Proof completed, 1800.)

(iii) *Theorematis arithmetici demonstratio nova* (Comm. Gött. xvi. (1808), or Werke, ii. p. 1).

(iv) *Summatio quarumdam serierum singularium*, Arts. 32—36. (Ibid. i. (new series) 1811, or Werke, ii. p. 11.)

(v) and (vi) *Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et ampliationes novæ.* (Ibid. iv. (new series) 1818, or Werke, ii. p. 49.)

(vii) and (viii) *Analysis Residuorum*, Arts. 365, 366. (Werke, ii. p. 233.)

Of more recent proofs, the most instructive are those of Eisenstein (Crelle, xxix. (1845), p. 177), Zeller (Berlin Monatsb. Dec. 1872), and Kronecker (Crelle, xcvi. (1884), p. 348, and xcvii. p. 93 ; also in the Berlin Monatsb. for 1884).

In the second volume of Gauss's collected works (p. 400) there is a table giving the value of $(p \mid q)$, where p, q are primes, from $p=2$ to $p=997$ and from $q=3$ to $q=503$.

CHAPTER III.

Binary Quadratic Forms; Analytical Theory.

48. A RATIONAL, integral, homogenous function of any number of variables is called an *algebraical form.* Forms are classified according to the number of variables as binary, ternary, etc., and according to their degree in the variables as linear, quadratic, cubic, and so on. It is convenient to speak of a 'cubic' instead of a 'cubic form,' and so in other cases. Thus

$$ax^3 + 3bx^2y + 3cxy^2 + dy^3$$

is a binary cubic;

$$ax^2 + by^2 + cz^2 + 2fyz + 2gzx + 2hxy$$

is a ternary quadratic. These forms are expressed more compactly by the notation $(a, b, c, d \between x, y)^3$, $(a, b, c, f, g, h \between x, y, z)^2$; as a matter of convenience the literal coefficients are understood to be multiplied by the corresponding numerical coefficients of the expansions of $(x + y)^3$ and $(x + y + z)^2$. So, in general, the m-ary n-tic may be written $(a, b, c \ldots \between x_1, x_2 \ldots x_m)^n$, where the literal coefficients are to be multiplied by the corresponding numerical coefficients in the expansion of $(x_1 + x_2 + x_3 + \ldots + x_m)^n$.

The suppression of the numerical multipliers is indicated by writing $(a, b, c \ldots \between x_1, x_2 \ldots)^n$. Thus $(a, b, c \between x, y)^2$ means

$$ax^2 + bxy + cy^2.$$

In the arithmetical theory of forms the coefficients, as well as the variables, are understood to be integers, unless the contrary is expressed.

Within the last fifty years, the algebraical theory of forms has developed into one of the most important branches of analysis. It may fairly be said that the germs of the modern algebra of linear substitutions and concomitants are to be found in the fifth section of the *Disquisitiones Arithmeticæ*; and inversely, every advance in the algebraic theory of forms is an acquisition to the arithmetical theory. At the same time, the additional difficulties which the latter involves are so serious that, except in the simplest case, that of binary quadratics, much remains to be done to advance it to the same relative degree of perfection.

49. For the present, our attention will be confined to binary quadratic forms with real integral coefficients. Many of the earlier arithmetical discoveries made in the interval extending from Diophantus to Euler may be expressed as theorems relating to certain special quadratic forms; thus the representation of a number as the sum of two squares is connected with the form $x^2 + y^2$. The general theory was first treated in a systematic way by Lagrange and Legendre, and afterwards more completely by Gauss in the *Disquisitiones Arithmeticæ*. Quite recently, new light has been shed on the properties of binary quadratic forms by the researches of Dedekind, Klein, Poincaré and others in connexion with elliptic modular-functions and the allied transcendents, such as Fuchsian functions. Nevertheless, Gauss's work will always remain classical, so that an account of the subject, principally from his point of view, with some simplifications due to Dirichlet, will naturally precede the discussion of later developments.

Throughout the rest of this chapter the word 'form' will be used in the sense of 'binary quadratic form with real integral coefficients.' When there is no reason to specify the variables, or indicate their connexion with other variables, (a, b, c) will be written for $ax^2 + 2bxy + cy^2$. Here a is called the first coefficient, b the second, and c the third. It is important to observe that the forms (a, b, c) and (c, b, a) are to be considered different (except when $c = a$) although the first becomes identical with the second, if the variables are interchanged.

Representation of Numbers.

50. A number m is said to be represented by a form (a, b, c), when numbers x, y can be found such that

$$ax^2 + 2bxy + cy^2 = m.$$

The representation is *primitive* or *derived* according as x, y are relatively prime or otherwise. It is clear that if $dv\,(x, y) = \mu$,[1] m is divisible by μ^2, and that if $x = \mu x'$, $y = \mu y'$, $ax'^2 + 2bx'y' + cy'^2$ is a primitive representation of m/μ^2. It will therefore only be necessary to consider primitive representations, and we may use 'represented' in the sense of 'primitively represented,' unless the contrary is expressed.

51. The properties of a form (a, b, c) are intimately connected with the value of its discriminant $ac - b^2$. This discriminant, *with its sign changed*, is called the *determinant* of the form, and generally denoted by D, so that $D = b^2 - ac$. One distinction between forms of a positive, and those of a negative determinant, immediately presents itself. Namely, if $m = ax^2 + 2bxy + cy^2$, we deduce $am = (ax + by)^2 - Dy^2$, $cm = (cy + bx)^2 - Dx^2$; so that if D is negative, am, cm are both positive for real values of x, y, and a, c, m have the same sign. That is, all numbers representable by a form (a, b, c) of a negative determinant, are of the same sign, that sign being the same as that of the first and third coefficients of the form. On the other hand, if D is positive, the form may be made to represent both positive and negative numbers. For in this case,

$$\begin{aligned} am &= (ax + by)^2 - Dy^2 \\ &= \{ax + (b + \sqrt{D})\,y\}\,\{ax + (b - \sqrt{D})\,y\}, \end{aligned}$$

and integral values of x, y can always be found so as to make the linear factors on the right agree or differ in sign. This is most easily seen by considering x, y as the rectangular coordinates of a point: for the two lines $ax + (b \pm \sqrt{D})\,y = 0$ will divide the plane of reference into four regions, each of which will contain points whose coordinates are integers. For points within two of these regions the values of $ax + (b + \sqrt{D})\,y$ and $ax + (b - \sqrt{D})\,y$ will agree in sign: for the other two they will differ. Hence by a suitable choice of the integers x, y, the value of am, and consequently of m, can be made positive or negative at pleasure.

Forms of negative determinant may be called *definite* forms, and further subdivided into positive and negative forms according as a, c are both positive or both negative. It is sufficient to consider positive forms, since the properties of negative forms may

[1] By $dv\,(x, y)$ is meant the greatest common measure of x and y, taken positively.

be immediately inferred. Forms for which D is positive are called *indefinite*.

In the special case when D is a positive square, k^2 suppose, the form $ax^2 + 2bxy + cy^2$ may be written

$$\frac{1}{a}\{ax + (b+k)y\}\{ax + (b-k)y\}.$$

Such forms will be excluded from the discussion; the theory of them presents no special difficulty or interest, and belongs more properly to that of linear forms.

52. In connexion with any form (a, b, c) we shall have to consider the quadratic equation

$$a\omega^2 + 2b\omega + c = 0.$$

The roots of this are

$$\omega_1 = \frac{-b+\sqrt{D}}{a}, \quad \omega_2 = \frac{-b-\sqrt{D}}{a},$$

where $\sqrt{D}$ means the positive square root of D, if D is positive; while if D is negative and equal to $-\Delta$, $\sqrt{D}$ means $i\sqrt{\Delta}$, where $\sqrt{\Delta}$ is taken positively. It is convenient to call ω_1, ω_2 the roots of the form; ω_1 may be distinguished as the first or principal root, ω_2 as the second root.

53. The form (a, b, c) is said to be *primitive* if $dv\ (a, b, c) = 1$; if $dv\ (a, b, c) = \mu$, the form is said to be derived from the primitive form $(a/\mu, b/\mu, c/\mu)$. Primitive forms are subdivided into properly and improperly primitive, according as $dv\ (a, 2b, c) = 1$ or 2 respectively. Thus $(1, 1, 3)$ is properly primitive, $(2, 1, 2)$ improperly primitive; $(2, 2, 6)$, $(6, 3, 6)$ are forms derived from them.

The determinant of a derived form necessarily involves a square factor.

For every determinant D there is at least one properly primitive form; in fact, $(1, 0, -D)$ is properly primitive, and is called the *principal* form of determinant D.

Improperly primitive forms exist only when $D \equiv 1 \pmod 4$. For if $dv\ (a, 2b, c) = 2$, it follows that a, c are even and b is odd, therefore $D = b^2 - ac \equiv 1 \pmod 4$. Conversely, if $D = 4n + 1$, the form $(2, 1, -2n)$ is improperly primitive, and of determinant D.

Transformation and Equivalence.

54. Suppose the variables x, y are connected with two other variables x', y' by means of the linear equations

$$x = \alpha x' + \beta y',$$
$$y = \gamma x' + \delta y',$$

where α, β, γ, δ are integers. If we substitute these values of x, y in the form $(a, b, c\between x, y)^2$ it becomes $(a', b', c'\between x', y')^2$, where

$$\begin{aligned} a' &= a\alpha^2 + 2b\alpha\gamma + c\gamma^2, \\ b' &= a\alpha\beta + b\,(\alpha\delta + \beta\gamma) + c\gamma\delta, \\ c' &= a\beta^2 + 2b\beta\delta + c\delta^2. \end{aligned}$$

We may say that the form (a, b, c) has been transformed into (a', b', c') by the substitution $\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}$: and the connexion between the old and the new variables may be expressed by writing

$$(x, y) = \left(\begin{matrix}\alpha, & \beta \\ \gamma, & \delta\end{matrix}\between x', y'\right).$$

Whenever x', y' are integers, x, y are so; therefore every number (primitively or otherwise) representable by (a', b', c') is representable by (a, b, c). On this account the form (a', b', c') is said to be contained in (a, b, c).

The integer $\alpha\delta - \beta\gamma = \epsilon$, say, is called the determinant of the substitution: and (a, b, c) is said to contain (a', b', c') properly or improperly, according as ϵ is positive or negative.

If $\epsilon = \pm 1$, the substitution may be called unitary; and proper or improper, according as $\epsilon = +1$ or -1.

Expressing x', y' in terms of x, y, we have

$$x' = (\delta x - \beta y)/\epsilon,$$
$$y' = (-\gamma x + \alpha y)/\epsilon.$$

In order that x', y' may be integers whenever x, y are so, it is necessary and sufficient that α/ϵ, β/ϵ, γ/ϵ, δ/ϵ should all be integers. Now

$$\frac{\alpha}{\epsilon}\cdot\frac{\delta}{\epsilon} - \frac{\beta}{\epsilon}\cdot\frac{\gamma}{\epsilon} = \frac{1}{\epsilon};$$

so that, in the case considered, $1/\epsilon$ is an integer: therefore $\epsilon = \pm 1$. Conversely, whenever $\epsilon = \pm 1$, each of the forms (a, b, c), (a', b', c')

is contained in the other, and they are said to be *equivalent*, properly or improperly, according as $\epsilon = +1$ or -1.

The proper equivalence of two forms (a, b, c) (a', b', c') may be indicated by the notation

$$(a, b, c) \sim (a', b', c').$$

55. It follows from the theory of invariants, or may be proved independently, that if (a, b, c) is transformed into (a', b', c') by the substitution $\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}$, then

$$\begin{aligned} D' = b'^2 - a'c' &= (b^2 - ac)(\alpha\delta - \beta\gamma)^2 \\ &= D\epsilon^2. \end{aligned}$$

If the two forms are equivalent, $\epsilon^2 = 1$, and therefore $D' = D$. It is not true, conversely, that if $D' = D$, the forms are equivalent; in fact, one of the fundamental problems to be solved is that of deciding whether two given forms of the same determinant are equivalent or not. Supposing that they are, there is the further question of finding all the substitutions which transform one into the other.

56. Let the form (a, b, c) be converted into (a', b', c') by the unitary substitution $\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}$ of determinant ϵ: and let ω_1, ω_2 be the roots of (a, b, c), ω_1', ω_2' those of (a', b', c'). Then if ω' is the root of (a', b', c') corresponding to ω_1,

$$\omega_1 = \frac{\alpha\omega' + \beta}{\gamma\omega' + \delta},$$

and therefore

$$\begin{aligned} \omega' = \frac{\delta\omega_1 - \beta}{-\gamma\omega_1 + \alpha} &= \frac{\delta(-b + \sqrt{D}) - \beta a}{-\gamma(-b + \sqrt{D}) + \alpha a} \\ &= \frac{\{a\alpha + b\gamma + \gamma\sqrt{D}\}\{-a\beta - b\delta + \delta\sqrt{D}\}}{(a\alpha + b\gamma)^2 - D\gamma^2} \\ &= \frac{-a\{a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta\} + a(\alpha\delta - \beta\gamma)\sqrt{D}}{a(a\alpha^2 + 2b\alpha\gamma + c\gamma^2)} \\ &= \frac{-b' + \epsilon\sqrt{D}}{a'}; \end{aligned}$$

consequently $\omega' = \omega_1'$ or ω_2' according as $\epsilon = +1$ or -1; that is, according as the forms are properly or improperly equivalent. This way of expressing the distinction between proper and improper equivalence is due to Dirichlet[1].

[1] *Berlin Abhandl.*, 1854, p. 99; *Liouville* (2nd series), vol. ii., p. 353.

57. Suppose that a form $f = ax^2 + 2bxy + cy^2$ is transformed into $f' = a'x'^2 + 2b'x'y' + c'y'^2$ by the substitution $S = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$, of determinant ϵ; and that f' is transformed into

$$f'' = a''x''^2 + 2b''x''y'' + y''^2$$

by the substitution $S' = \begin{pmatrix} \alpha', & \beta' \\ \gamma', & \delta' \end{pmatrix}$, of determinant ϵ'.

Then since

$$\begin{aligned} x &= \alpha x' + \beta y' \\ &= \alpha(\alpha' x'' + \beta' y'') + \beta(\gamma' x'' + \delta' y'') \\ &= (\alpha\alpha' + \beta\gamma') x'' + (\alpha\beta' + \beta\delta') y'' \end{aligned}$$

and similarly $\quad y = (\gamma\alpha' + \delta\gamma') x'' + (\gamma\beta' + \delta\delta') y''$,

it is clear that f is transformed into f'' by the substitution

$$\begin{pmatrix} \alpha\alpha' + \beta\gamma', & \alpha\beta' + \beta\delta' \\ \gamma\alpha' + \delta\gamma', & \gamma\beta' + \delta\delta' \end{pmatrix}.$$

This substitution is said to be compounded of S and S', and is denoted by SS'. It is to be carefully observed that

$$S'S = \begin{pmatrix} \alpha'\alpha + \beta'\gamma, & \alpha'\beta + \beta'\delta \\ \gamma'\alpha + \delta'\gamma, & \gamma'\beta + \delta'\delta \end{pmatrix}$$

is, in general, different from SS'.

In forming the elements of SS' we proceed in the same way as in the multiplication of the determinants $\begin{vmatrix} \alpha, & \beta \\ \gamma, & \delta \end{vmatrix}$, $\begin{vmatrix} \alpha', & \beta' \\ \gamma', & \delta' \end{vmatrix}$, the multiplication being performed according to rows of the first matrix and columns of the second.

The determinant of SS' is

$$\begin{aligned} (\alpha\alpha' + \beta\gamma')(\gamma\beta' + \delta\delta') - (\alpha\beta' + \beta\delta')(\gamma\alpha' + \delta\gamma') \\ = (\alpha\delta - \beta\gamma)(\alpha'\delta' - \beta'\gamma') \\ = \epsilon\epsilon'. \end{aligned}$$

This is positive or negative according as ϵ, ϵ' agree or differ in sign; therefore SS' is a proper substitution if S, S' are both proper or both improper; otherwise it is improper.

We may compound SS' with any other substitution S'' and thus obtain $(SS')S''$. It may easily be verified and is, in fact, obvious that this is the same as $S(S'S'')$, so that it may be expressed without ambiguity by $SS'S''$; and, in general, the result of compounding any number of substitutions $S_1, S_2, \ldots S_n$, in this order, may be written $S_1 S_2 \ldots S_n$, and called the product of the substitutions (in this order). In particular, a substitution may be compounded with itself any number of times and the result written in the form S^p.

The substitution $\begin{pmatrix}1, & 0\\ 0, & 1\end{pmatrix}$ leaves the variables unaltered; it is called the identical substitution, and may be denoted by **1**.

Let $S=\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ be a unitary substitution, so that $\epsilon^2=1$. We have

$$\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}\begin{pmatrix}\delta/\epsilon, & -\beta/\epsilon\\ -\gamma/\epsilon, & \alpha/\epsilon\end{pmatrix}=\begin{pmatrix}(\alpha\delta-\beta\gamma)/\epsilon, & 0\\ 0 & , (\alpha\delta-\beta\gamma)/\epsilon\end{pmatrix}$$
$$=\begin{pmatrix}1, & 0\\ 0, & 1\end{pmatrix}=1.$$

The substitution $S'=\begin{pmatrix}\delta/\epsilon, & -\beta/\epsilon\\ -\gamma/\epsilon, & \alpha/\epsilon\end{pmatrix}$ is said to be inverse to S, and is denoted by S^{-1}. Evidently $(S^{-1})^{-1}=S$, and $S^{-1}S=SS^{-1}=1$. We may also write S^{-n} for $(S^{-1})^n$, where n is a positive integer; and it is clear that $S^{-n}=(S^n)^{-1}$; for instance,

$$S^3 . S^{-3}=S^2 . SS^{-1} . S^{-2}=S^2S^{-2}=S . SS^{-1} . S^{-1}=SS^{-1}=1,$$

and so in general. Thus for all positive and negative integral indices, $S^mS^n=S^{m+n}$; and after the admission of negative indices it still remains true that in the composition of substitutions the associative law of algebraical multiplication is valid, but not the commutative.

58. Applying these results to the theory of quadratic forms, we draw the following conclusions:—

I. If $f_1, f_2 \dots f_n$ be any number of forms each of which contains the next following, f_1 will contain f_n; and a substitution which transforms f_1 into f_n may be obtained by compounding the substitutions which convert f_1 into f_2, f_2 into $f_3 \dots f_{n-1}$ into f_n. The resulting substitution is proper or improper according as the number of its improper components is even or odd.

II. If f_1, f_2, f_3 are any three forms, such that f_1 is equivalent to f_2, and f_2 to f_3, then f_1 is equivalent to f_3.

In particular, if $f_1 \sim f_2$, and $f_2 \sim f_3$, then $f_1 \sim f_3$.

For the present only proper equivalence will be considered, and 'equivalent' will be used in the sense of 'properly equivalent.' Similarly 'unitary substitution' will mean 'proper unitary substitution,' unless the contrary is stated

Reduction of the problem of representation to that of equivalence.

59. It has already been observed (see above, Art. 50) that in discussing the representation of numbers it is sufficient to consider primitive representations. Suppose, now, that

$$m = a\alpha^2 + 2b\alpha\gamma + c\gamma^2$$

is a primitive representation of an integer m by the form (a, b, c), so that α, γ are integers prime to each other. Let integers β, δ be chosen such that $\alpha\delta - \beta\gamma = 1$. Then the substitution $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ converts (a, b, c) into an equivalent form (a', b', c'), where

$$a' = a\alpha^2 + 2b\alpha\gamma + c\gamma^2 = m,$$
$$b' = a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta = n, \text{ say},$$
$$c' = a\beta^2 + 2b\beta\delta + c\delta^2 = l.$$

Conversely, if we can find a form (m, n, l) equivalent to (a, b, c) and if $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ is any unitary substitution which converts (a, b, c) into (m, n, l), then m may be represented in the form $(a, b, c \between x, y)^2$ by putting $x = \alpha$, $y = \gamma$.

Since
$$n^2 - lm = D,$$
it follows that
$$n^2 \equiv D \pmod{m},$$
and therefore D is a quadratic residue of m. Hence no number of which D is a non-residue can be represented by any form of which the determinant is D. On the other hand, if m is any number of which D is a residue, and n a root of the congruence $n^2 \equiv D \pmod{m}$, then $(n^2 - D)/m$ is an integer, l suppose, and the form (m, n, l) is of determinant D, and one by which m can be represented.

If $\pm n$, $\pm n'$, $\pm n''$, etc. are all the incongruous solutions of $n^2 \equiv D \pmod{m}$, and l, l', l'', etc. the corresponding values of $(n^2 - D)/m$, every form (a, b, c) of determinant D by which m can be represented must be equivalent to one of the forms

$$(m, n, l), (m, -n, l), (m, n', l'), (m, -n', l') \text{ etc.}$$

Conversely m can be represented by any form which is equivalent to one of these.

When α, γ are given, the general values of β, δ are of the form

$$\beta = \beta_0 + k\alpha, \quad \delta = \delta_0 + k\gamma,$$

k being any integer, and β_0, δ_0 two particular values of β, δ so that $\alpha\delta_0 - \beta_0\gamma = 1$. Hence the general value of n is

$$\begin{aligned} n &= (a\alpha + b\gamma)\beta + (b\alpha + c\gamma)\delta \\ &= (a\alpha + b\gamma)\beta_0 + (b\alpha + c\gamma)\delta_0 \\ &\qquad + k(a\alpha^2 + 2b\alpha\gamma + c\gamma^2) \\ &= n_0 + km \equiv n_0 \pmod{m}, \end{aligned}$$

n_0 being a particular value of n.

The representation $m = a\alpha^2 + 2b\alpha\gamma + c\gamma^2$ is said to appertain to the root n_0 of the congruence $n^2 \equiv D \pmod{m}$. Representations appertaining to the same root of the congruence are said to belong to the same set.

We shall return to the problem of representation later on: meanwhile, enough has been said to shew its dependence upon the theory of equivalence, which will now be considered in detail.

60. Before doing so, however, it may be well to give an outline of the principal results which will be obtained.

Forms which are properly equivalent are said to belong to the same *class*. Each class contains an infinite number of forms, any one of which may be taken as a representative of the class; all the other forms of the class being derivable from it by means of unitary substitutions.

For every determinant the number of distinct classes is finite. The proof of this fundamental proposition consists in shewing that for any given determinant there exists a limited number of forms, called *reduced* forms, the coefficients of which satisfy certain conditions of inequality, and that each class contains at least one reduced form. The criteria of a reduced form are quite distinct for definite and indefinite forms; but in each case we are able to construct a complete system of reduced forms and to arrange them into sets of equivalent forms. The number of sets is equal to the number of classes for the determinant considered.

A method is devised by which any proposed form may be transformed into an equivalent reduced form; so that in order to find out whether two given forms of the same determinant are equivalent or not, it is sufficient to find reduced forms equivalent to them, and then decide whether these reduced forms belong to the same class. This can be done in every case; and moreover, if the two given forms are equivalent, the process by which this fact is established also enables us to find a unitary substitution which will convert one of the forms into the other.

Finally, by a method which is applicable to all quadratic forms, we are able to find all the substitutions by which a given form may be converted into another given form which is equivalent to it.

61. Let the form $f=(a, b, c)$ be transformed into the equivalent form $f'=(a', b', c')$ by the proper unitary substitution $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$: then (Art. 54)

$$\begin{aligned}a' &= a\alpha^2 + 2b\alpha\gamma + c\gamma^2\\ b' &= a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta\\ c' &= a\beta^2 + 2b\beta\delta + c\delta^2.\end{aligned}$$

From this it is evident that every common divisor of a, b, c is also a common divisor of a', b', c'. Now since f' is converted into f by the inverse substitution $\begin{pmatrix}\delta, & -\beta\\ -\gamma, & \alpha\end{pmatrix}$, a, b, c can be expressed as integral linear functions of a', b', c'; therefore every common divisor of a', b', c' is also a common divisor of a, b, c. Therefore

$$dv\,(a', b', c') = dv\,(a, b, c)$$

and similarly $$dv\,(a', 2b', c') = dv\,(a, 2b, c).$$

That is to say, f and f' are either both properly primitive, or both improperly primitive, or both derived forms; and moreover in the last case they are derived from equivalent primitive forms.

Classes, therefore, like forms, may be distributed into primitive and derived classes.

Any two forms (a, b, c) (a', b', c') of the same determinant are said to belong to the same *order* if $dv\,(a', b', c') = dv\,(a, b, c)$ *and* $dv\,(a', 2b', c') = dv\,(a, 2b, c)$. There is a corresponding arrangement of classes; so that we may have, in the most general case, orders of properly primitive classes, of improperly primitive classes, and of classes derived from properly and improperly primitive classes respectively.

In the theory of equivalence it is sufficient to consider primitive forms; and in like manner with regard to the representation of numbers. For it follows from the results of this article that every form equivalent to $(\mu a, \mu b, \mu c)$ must be of the type $(\mu a', \mu b', \mu c')$, and from the equivalence $(\mu a', \mu b', \mu c') \backsim (\mu a, \mu b, \mu c)$ we infer $(a', b', c') \backsim (a, b, c)$. Similarly if m is representable by a derived form $(\mu a, \mu b, \mu c)$, m/μ must be an integer, and to every representation of m by $(\mu a, \mu b, \mu c)$ corresponds a representation of m/μ by (a, b, c) and conversely. In what follows, therefore, unless the contrary is stated, it will be supposed that the forms considered are primitive.

62. A good deal of brevity and clearness is gained by adopting the following definitions.

Two forms (a, b, c), $(a, -b, c)$, which differ only in the sign of their middle coefficients, are said to be *opposite* forms. Opposite forms are always improperly equivalent, for the substitution $\begin{pmatrix}1, & 0\\ 0, & -1\end{pmatrix}$ converts (a, b, c) into $(a, -b, c)$.

Two forms are *adjacent*, when the first coefficient of one is equal to the third coefficient of the other, and moreover this common coefficient divides the sum of the middle coefficients. Or, in symbols, the forms are (a, b, a'), (a', b', a''), with $b + b' \equiv 0 \pmod{a'}$. Two adjacent forms are properly equivalent; for if we put $(b + b')/a' = -\delta$, it is easily verified that the substitution $\begin{pmatrix}0, & 1\\ -1, & \delta\end{pmatrix}$ converts (a, b, a') into (a', b', a''). It may be observed also that

$$a'' = \frac{b'^2 - D}{a'} = \frac{(b^2 - D) - (b + b')(b - b')}{a'}$$

$$= a + \delta(b - b').$$

A special case which should be noted is that $(c, -b, a) \backsim (a, b, c)$, the substitution which converts one of these forms into the other being $\begin{pmatrix}0, & 1\\ -1, & 0\end{pmatrix}$.

An *ambiguous* form is one for which the double of the middle coefficient is divisible by the first; that is, (a, b, c) is ambiguous if $2b \equiv 0 \pmod{a}$. An ambiguous form is properly equivalent to its opposite; for if $2b = -\beta a$, the substitution $\begin{pmatrix}1, & \beta\\ 0, & 1\end{pmatrix}$ converts (a, b, c) into $(a, -b, c)$. In particular, the principal form $(1, 0, -D)$ is ambiguous, and is also its own opposite; as, in fact, are all forms with a zero middle coefficient.

Reduction of Definite Forms.

63. Consider a definite form (a, b, a') of determinant

$$D = b^2 - aa' = -\Delta,$$

a negative integer; and for simplicity, suppose that a, a' are positive. By the substitution $\begin{pmatrix} 0, & 1 \\ -1, & \delta \end{pmatrix}$ it is transformed into the adjacent form (a', b', a''), where

$$b' = -b - a'\delta$$
$$a'' = a + \delta(b - b').$$

Now let δ be chosen so that $2|b'| \not> a'$: this can always be done, and in general in one way only; namely b' is the absolutely least residue of $-b$ (mod a'), and δ is determined by $\delta = -(b + b')/a$. The only exceptional case is when $b \equiv \frac{1}{2}a'$ (mod a'), a' being even; here we may take $b' = +\frac{1}{2}a'$ or $-\frac{1}{2}a'$ (cf. Art. 9). If $a'' < a'$, we can transform (a', b', a'') in the same way into (a'', b'', a'''), where $2|b''| \not> a''$; and if $a''' < a''$, the process may be repeated. We must at last arrive at a form (A, B, C) for which $2|B| \not> A$, and $C \not< A$: because the series of continually diminishing positive integers $a', a'', a''' \ldots$ cannot go on indefinitely.

A positive form (A, B, C) *of this kind, for which*

$$C \not< A \not< 2|B|,$$

is called a reduced form.

It follows from what has been previously proved that a reduced form equivalent to any given positive form can always be found. The process of reduction leads to a set of successive substitutions $\begin{pmatrix} 0, & 1 \\ -1, & \delta \end{pmatrix}$, $\begin{pmatrix} 0, & 1 \\ -1, & \delta' \end{pmatrix}$, etc., and to a corresponding set of forms, each of which is adjacent to the next following. The first form of the set is the given form, and the last is reduced; so that by compounding the successive substitutions, we obtain a substitution by which the given form is converted into a reduced form.

As an illustration, let the form be (10, 17, 29); then the series of equivalent forms deduced from it is

$$(10, 17, 29), (29, 12, 5), (5, -2, 1), (1, 0, 1),$$

of which the last is reduced. The successive substitutions are $\begin{pmatrix} 0, & 1 \\ -1, & -1 \end{pmatrix}$, $\begin{pmatrix} 0, & 1 \\ -1, & -2 \end{pmatrix}$, $\begin{pmatrix} 0, & 1 \\ -1, & 2 \end{pmatrix}$; and by compounding these we obtain $\begin{pmatrix} 2, & -5 \\ -1, & 3 \end{pmatrix}$, by means of which (10, 17, 29) is transformed into (1, 0, 1).

Or, again, let the form be (29, 51, 90): then the series of forms is

$$(29, 51, 90), (90, 39, 17), (17, -5, 2), (2, \pm 1, 5),$$

where the forms (2, 1, 5) and (2, − 1, 5) are both reduced.

If ω_1, ω_2 are the roots of $A\omega^2 + 2B\omega + C = 0$, the conditions that (A, B, C) may be a reduced form are equivalent to $|\omega_1 + \omega_2| \not> 1$, $|\omega_1 \omega_2| \not< 1$. Observe that since ω_1, ω_2 are conjugate complex quantities, $|\omega_1| = |\omega_2|$, so that the second condition may be replaced by $|\omega_1| \not< 1$. The significance of this will be seen later on.

64. *For a given negative determinant, the number of reduced forms is finite.*

Let (A, B, C) be a reduced positive form for the determinant $D = -\Delta$; then $\Delta = AC - B^2$. The conditions of reduction being $2|B| \not> A$, and $C \not< A$, we have $AC \not< A^2$, and $B^2 \not> \frac{1}{4}A^2$; hence $\Delta = AC - B^2 \not< \frac{3}{4}A^2$, or $A \not> \sqrt{\frac{4}{3}\Delta}$. Hence also $|B| \not> \sqrt{\frac{1}{3}\Delta}$, and $AC = \Delta + B^2 \not> \frac{4}{3}\Delta$, so that $C \not> \frac{4}{3}\Delta$. The values of A, B, C being all limited, it follows that the number of reduced positive forms is finite.

From each positive reduced form (A, B, C) we obtain a corresponding negative reduced form $(-A, B, -C)$ by changing the sign of the extreme coefficients.

In order to construct a complete set of reduced forms for the determinant $-\Delta$, we take $B = 0, \pm 1, \pm 2, \dots \pm \lambda$, where λ is the greatest integer contained in $\sqrt{\frac{1}{3}\Delta}$; then, attributing to B any one of these values, we break up $\Delta + B^2$ in all possible ways into the product of two integral factors A, C: finally, we reject those combinations for which the conditions $|C| \not< |A| \not< 2|B|$ are not satisfied. The remaining sets (A, B, C) give reduced forms.

Example 1. Suppose $\Delta = 40$. Here $\sqrt{40/3}$ is between 3 and 4, so that $\lambda = 3$, and the calculation is as follows :—

$B = 0$	$AC = 1.40,\ 2.20,\ 4.10,\ 5.8,$
± 1	$1.41^*,$
± 2	$1.44^*,\ 2.22^*,\ 4.11,$
± 3	$1.49^*,\ 7.7.$

The decompositions marked with an asterisk have to be rejected: so that the positive reduced forms are

$$(1,\ 0,\ 40),\ (2,\ 0,\ 20),\ (4,\ 0,\ 10),\ (5,\ 0,\ 8),$$
$$(4,\ \pm 2,\ 11),\ (7,\ \pm 3,\ 7);$$

eight in all.

It is to be observed that this process gives the derived as well as the primitive forms; thus, in the above example, (2, 0, 20) and (4, 0, 10) are derived forms.

Example 2. $\Delta = 39, \quad \lambda = 3,$

$B = 0 \qquad AC = 1\,.\,39,\ 3\,.\,13,$

$\pm 1 \qquad 1\,.\,40^*,\ 2\,.\,20,\ 4\,.\,10,\ 5\,.\,8,$

$\pm 2 \qquad 1\,.\,43^*,$

$\pm 3 \qquad 1\,.\,48^*,\ 2\,.\,24^*,\ 3\,.\,16^*,\ 4\,.\,12^*,\ 6\,.\,8.$

The reduced positive forms are:

(i) properly primitive, (1, 0, 39), (3, 0, 13), (5, ± 1, 8):

(ii) improperly primitive, (2, ± 1, 20), (4, ± 1, 10), (6, ± 3, 8).

65. We have now to inquire whether two positive reduced forms (a, b, c), (a', b', c') of the determinant $-\Delta$ can be properly equivalent. Suppose that the substitution $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ converts (a, b, c) into (a', b', c'). Then

$$aa' = a(a\alpha^2 + 2b\alpha\gamma + c\gamma^2) = (a\alpha + b\gamma)^2 + \Delta\gamma^2 \not< \Delta\gamma^2.$$

Now $aa' \not> \frac{4}{3}\Delta$, and γ is an integer: therefore $\gamma^2 = 0$ or 1.

Similarly, by considering the inverse substitution $\begin{pmatrix}\delta, & -\beta\\ -\gamma, & \alpha\end{pmatrix}$ which converts (a', b', c') into (a, b, c), we conclude that $\beta^2 = 0$ or 1.

If $\beta = \gamma = 0$, $\alpha = \delta = \pm 1$ and the forms are identical.

Next suppose $\gamma = 0$, $\beta = \pm 1$; then

$$\alpha = \delta = \pm 1,\ a' = a,\ b' = b \pm a.$$

The conditions of reduction $2|b| \not> a$, $2|b'| \not> a'$, cannot both be satisfied unless $b = \pm \frac{1}{2}a$, $b' = \mp \frac{1}{2}a$. The forms $(a, \frac{1}{2}a, c)$, $(a, -\frac{1}{2}a, c)$ are in fact equivalent, the first being converted into the second by the substitution $\begin{pmatrix}1, & -1\\ 0, & 1\end{pmatrix}$.

Suppose $\gamma = \pm 1$, $\beta = 0$. This is merely the inverse of the preceding, and leads to the same result.

Next, let $\gamma = \pm 1$, $\beta = \mp 1$; then $\alpha\delta = 0$. If $\alpha = 0$,

$$\begin{aligned} a' &= c, \\ b' &= -b \pm c\delta, \\ c' &= a \mp 2b\delta + c\delta^2. \end{aligned}$$

The conditions $2|b| \ngtr a$, $2|b'| \ngtr a'$ cannot both be satisfied, except in the two following cases:—

(i) $\delta = 0$. The forms in this case are (a, b, a), $(a, -b, a)$, which are obviously equivalent, the transforming substitution being $\begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}$.

(ii) $\delta = \pm 1$. Here $2|b'| > c$, except when $c = a$, and

$$b' = -b = \pm \tfrac{1}{2}a.$$

The forms are $(a, \frac{1}{2}a, a)$ and $(a, -\frac{1}{2}a, a)$, of which the first may be converted into the second by the transformations $\begin{pmatrix} 1, & -1 \\ 0, & 1 \end{pmatrix}$ and $\begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}$.

The case where $\beta = \pm 1$, $\gamma = 0$ leads to the same result.

Finally, let $\beta = \gamma = \pm 1$; then $\alpha\delta = 2$, so that either $\alpha = \pm 2$, $\delta = \pm 1$, or $\alpha = \pm 1$, $\delta = \pm 2$.

Suppose $\alpha = 2$, $\delta = 1$. Then by the equations of transformation,

$$\begin{aligned} a' &= 4a \pm 4b + c, \\ c' &= a \pm 2b + c; \end{aligned}$$

therefore

$$a' - c' = 3a \pm 2b,$$

which is positive; hence $a' > c'$, and the form (a', b', c') cannot be reduced.

The other cases may be treated in the same way: and the conclusion is that

the only possible pairs of equivalent reduced forms are $(a, \frac{1}{2}a, c)$, $(a, -\frac{1}{2}a, c)$ *and* (a, b, a), $(a, -b, a)$; *with* $(a, \frac{1}{2}a, a)$, $(a, -\frac{1}{2}a, a)$ *belonging, as it were, to both cases.*

66. From every such pair of equivalent reduced forms we reject that form of which the middle coefficient is negative. The remaining forms are all non-equivalent, and may be taken as representatives of the different classes for the given determinant.

Thus, for instance, when $\Delta = 39$, we reject one of each of the pairs $(2, \pm 1, 20)$ and $(6, \pm 3, 8)$: there remain eight representative forms, four properly primitive,

$$(1, 0, 39),\ (3, 0, 13),\ (5, 1, 8),\ (5, -1, 8),$$

and four improperly primitive,

$$(2, 1, 20),\ (6, 3, 8),\ (4, 1, 10),\ (4, -1, 10).$$

Similarly when $\Delta = 40$ the equivalent pairs are $(4, \pm 2, 11)$ and $(7, \pm 3, 7)$, and we may take as representative forms

$$(1, 0, 40),\ (5, 0, 8),\ (4, 2, 11),\ (7, 3, 7);$$

$$(2, 0, 20),\ (4, 0, 10).$$

In order to discover whether two given definite forms are equivalent, we find, by the process of Art. 63, a reduced form equivalent to each. The necessary and sufficient condition for the equivalence of the proposed forms is that these reduced forms should either be identical, or form one of the special pairs of equivalent reduced forms.

Reduction of Indefinite Forms.

67. When the form (a, b, c) is indefinite, the roots of the equation $a\omega^2 + 2b\omega + c = 0$ are both real. The process of reduction is quite different from that employed for definite forms, and is closely connected with the expansion of a root of the equation in the form of a periodic chain-fraction.

As a first step, we observe that for a given positive determinant D there is only a limited number of forms (a, b, c) in which a, c have opposite signs. For if $(\pm a, b, \mp c)$ be such a form, $b^2 + ac = D$, and hence $|b| < \sqrt{D}$: also $ac = D - b^2 \not> D$, so that neither $|a|$ nor $|c|$ can exceed D.

Again, it is sufficient to consider those forms for which b is positive, since the form $(a, -b, c) \backsim (c, b, a)$, being transformed into it by $\begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix}$.

We might consider all forms to be reduced for which b is positive and a, c have opposite signs. It is more convenient, however, to adopt Gauss's definition of a reduced form, which is as follows:—

An indefinite form (A, B, C), *of determinant* D, *is reduced if* B *is positive* (*not zero*) *and less than* $\sqrt{D}$, *and moreover*

$$\sqrt{D} - B < |A| < \sqrt{D} + B.$$

The following consequences of the definition should be noticed.

I. Since $B < \sqrt{D}$, $B^2 - D = AC$ is negative, so that A, C are of opposite signs.

II. We have $(\sqrt{D} - B)(\sqrt{D} + B) = -AC = |A|\,|C|$; and it follows from this and the conditions of inequality satisfied by $|A|$ that $\sqrt{D} + B > |C| > \sqrt{D} - B$: that is, $|A|$, $|C|$ satisfy the *same* conditions of inequality.

III. The roots of $A\omega^2 + 2B\omega + C = 0$ are

$$\omega_1 = \frac{-B + \sqrt{D}}{A}, \text{ a proper fraction, and}$$

$$\omega_2 = \frac{-B - \sqrt{D}}{A}, \text{ an improper fraction;}$$

moreover $\omega_1\omega_2 = C/A$, which is negative, so that ω_1, ω_2 differ in sign.

Conversely, if ω_1, ω_2 are of opposite signs, and $|\omega_1| < 1$, $|\omega_2| > 1$, the form is reduced; for these conditions require that $-B + \sqrt{D}$ and $-B - \sqrt{D}$ should have opposite signs, and that $-B - \sqrt{D}$ should be the greater numerically; hence B is positive and less than $\sqrt{D}$. Also since $|\omega_1| < 1$, $\sqrt{D} - B < |A|$, and since $|\omega_2| > 1$, $\sqrt{D} + B > |A|$.

IV. Since $|A| < \sqrt{D} + B$, and $B < \sqrt{D}$, it follows that

$$|A| < 2\sqrt{D};$$

and similarly

$$|C| < 2\sqrt{D}.$$

68. It is easy to construct a complete system of reduced forms for any given determinant. To do so, we assign to B all positive integral values (zero excluded) which are less than $\sqrt{D}$: taking any value, say B, we break up $D - B^2$ in all possible ways into the product of two positive factors A, C, and reject those combinations for which the condition that A, C shall each fall within the limits $\sqrt{D} - B$ and $\sqrt{D} + B$ is not satisfied. Each remaining combination gives, in general, four reduced forms

$(A, B, -C)$, $(-A, B, C)$, $(C, B, -A)$, $(-C, B, A)$; there are, of course, only two if $C = A$.

Thus if $D = 13$, the work will be as follows:—

$$\begin{array}{ll} B = 1 & AC = 1 \,.\, 12^*,\ 2 \,.\, 6^*,\ 3 \,.\, 4, \\ \phantom{B = {}}2 & \phantom{AC = {}}1 \,.\ \ 9^*,\ 3 \,.\, 3, \\ \phantom{B = {}}3 & \phantom{AC = {}}1 \,.\ \ 4\ ,\ 2 \,.\, 2. \end{array}$$

Since $\sqrt{D}$ lies between 3 and 4, the combinations marked with an asterisk have to be rejected: the complete system of reduced forms is therefore

$$(\pm 3,\ 1,\ \mp 4),\quad (\pm 4,\ 1,\ \mp 3),\quad (\pm 3,\ 2,\ \mp 3),$$
$$(\pm 1,\ 3,\ \mp 4),\quad (\pm 4,\ 3,\ \mp 1),\quad (\pm 2,\ 3,\ \mp 2);$$

twelve in all.

69. *A reduced form can always be found which is equivalent to any proposed form.*

This will be proved by showing that every form (a, b, a') is equivalent to a form (A, B, C) for which

$$\sqrt{D} - |A| < B < \sqrt{D},$$
$$|C| \not< |A|.$$

A form which satisfies these conditions of inequality is reduced, according to definition. For since $\sqrt{D} - B < |A|$, and

$$|D - B^2| = |A|\,|C|,$$

it follows that

$$|\sqrt{D} + B| > |C| > |A| > \sqrt{D} - B.$$

Hence B is *positive* and $< \sqrt{D}$, and moreover

$$\sqrt{D} + B > |A| > \sqrt{D} - B:$$

that is, (A, B, C) is reduced.

Let δ, b' be chosen so that

$$b + b' = -\delta a',$$
$$\sqrt{D} - |a'| < b' < \sqrt{D}.$$

This can be done in one way, and one only: for if λ be the greatest integer in $\sqrt{D}$ there is one and only one integer b' in the interval $(\lambda + 1 - |a'|, \lambda)$ which is congruent to $-b \pmod{a'}$. Choosing this, and putting $-(b + b')/a' = \delta$, the substitution $\begin{pmatrix} 0, & 1 \\ -1, & \delta \end{pmatrix}$ changes (a, b, a') into the adjacent form (a', b', a''), with $\sqrt{D} - |a'| < b' < \sqrt{D}$.

If $|a'| > |a''|$, the process can be repeated; and it follows, as in Art. 63, that after a finite number of operations we must arrive at a form (A, B, C) for which all the inequalities are satisfied.

For example, let the form be (76, 29, 11). Here $D = 5$, $\lambda = 2$, and the process of reduction leads to the series of forms

$$(76,\ 29,\ 11),\quad (11,\ -7,\ 4),\quad (4,\ -1,\ -1),\quad (-1,\ 1,\ 4),$$

of which the last is reduced.

The reducing substitutions are

$$\begin{pmatrix} 0, & 1 \\ -1, & -2 \end{pmatrix},\quad \begin{pmatrix} 0, & 1 \\ -1, & 2 \end{pmatrix},\quad \begin{pmatrix} 0, & 1 \\ -1, & 0 \end{pmatrix},$$

and by compounding these we obtain $\begin{pmatrix} -2, & -1 \\ 5, & 2 \end{pmatrix}$, by means of which (76, 29, 11) is converted into $(-1, 1, 4)$.

70. The next thing to be done is to find out which of the reduced forms are equivalent. To this end, we require the following proposition:—

If (a, b, a') is a reduced form, there exists one, and only one adjacent reduced form (a', b', a'') which is equivalent to it, and has its first coefficient equal to a'.

Suppose, in the first place, that a is positive: and let us write $-a'$ instead of a', since the third coefficient must be negative (Art. 67). Let δ, b' be chosen so that

$$b + b' = \delta a',$$
$$\sqrt{D} - a' < b' < \sqrt{D}.$$

This can be done in one way only: and moreover the value of b' thus obtained will be positive. For if b' were negative we should have $\sqrt{D} < a'$, and hence $b < a'$ and positive: the algebraically greatest negative value of b' is therefore $-b$ (corresponding to $\delta = 0$). But since $(a, b, -a')$ is reduced,

$$\sqrt{D} - b < a' < \sqrt{D} + b,$$

and therefore $-b < \sqrt{D} - a'$; that is, the algebraically greatest possible negative value of b' is less than $\sqrt{D} - a'$, contrary to the conditions of inequality by which b' is determined.

Since b' is positive, δ is positive and not zero; hence

$$\sqrt{D} + b' = \sqrt{D} - b + \delta a' > a',$$

and therefore the substitution $\begin{pmatrix} 0, & 1 \\ -1, & \delta \end{pmatrix}$ converts $(a, b, -a')$ into a form (a', b', a'') which is reduced.

In a similar way, from a reduced form $(-a, b, a')$ of which the first coefficient is negative, we may derive an adjacent reduced form $(a', b', -a'')$. Namely, if we determine δ, b' by

$$b + b' = -\delta a',$$
$$\sqrt{D} - a' < b' < \sqrt{D},$$

it can be proved as before that b' is positive; hence δ is negative and not zero, and therefore $\sqrt{D} + b' = \sqrt{D} - b - \delta a' > a'$, so that the substitution $\begin{pmatrix} 0, & 1 \\ -1, & \delta \end{pmatrix}$ converts $(-a, b, a')$ into a reduced form $(a', b', -a'')$.

71. Starting, now, with any reduced form (a, b, a'), we deduce in this way a series of reduced forms (a', b', a''), (a'', b'', a''') etc., each of which is equivalent to the one before it. The total number of reduced forms being finite, we must at last arrive at a form identical with (a, b, a'). In this way we obtain a cycle or *period* of reduced forms

$$(a, b, a'), (a', b', a'') \ldots (a^{(n-1)}, b^{(n-1)}, a).$$

If these forms are supposed to be arranged in a ring, each form will be connected with two adjacent forms, one following, and one preceding it; thus (a, b, a') is followed by (a', b', a'') and preceded by $(a^{(n-1)}, b^{(n-1)}, a)$.

The number of forms in a period is necessarily even, because the final coefficients a', a'', a''' ... are alternately positive and negative, and the last of these, namely $a^{(n)} = a$, has a sign opposite to that of a'.

After completing one period, we may take any one of the reduced forms which are left, and form its period; and so on. Finally, all the reduced forms will be arranged in a finite number of periods, each containing an even number of forms.

Thus for $D = 13$ the periods are

I. $(1, 3, -4), (-4, 1, 3), (3, 2, -3),$
$(-3, 1, 4), (4, 3, -1), (-1, 3, 4),$
$(4, 1, -3), (-3, 2, 3), (3, 1, -4),$
$(-4, 3, 1).$

II. $(2, 3, -2), (-2, 3, 2).$

72. Each form of a period, such as $(\pm a, b, \mp a')$, is transformed into the next following, $(\mp a', b', \pm a'')$, by means of a substitution $\begin{pmatrix} 0, & 1 \\ -1, & \delta \end{pmatrix}$. If ω, ω' are two corresponding roots of the forms,

$$\omega = \frac{1}{\delta - \omega'}.$$

Suppose, in particular, that ω is the principal root of its form: that is, let $\omega = \omega_1 = \frac{-b+\sqrt{D}}{\pm a}$; then when the upper sign is taken for $\pm a$, δ is positive, ω is a positive proper fraction, and

$$\omega = \frac{1}{\delta - \omega'} = \frac{1}{\delta + |\omega'|},$$

since $\omega' = \frac{-b'+\sqrt{D}}{-a'}$, which is negative.

If we take the lower sign for $\pm a$, ω is a negative proper fraction, δ is negative, and we have

$$|\omega| = -\omega = \frac{1}{-\delta + \omega'}$$

$$= \frac{1}{|\delta| + |\omega'|},$$

since ω' is positive.

In every case, therefore,

$$|\omega| = \frac{1}{|\delta| + |\omega'|}.$$

Similarly, if $\begin{pmatrix} 0, & 1 \\ -1, & \delta' \end{pmatrix}$ is the substitution which converts $(\mp a', b', \pm a'')$ into the next form of the period,

$$|\omega'| = \frac{1}{|\delta'| + |\omega''|},$$

and so on.

Hence, if $\phi_1, \phi_2 \dots \phi_{2m}$ are the forms of a period, $\begin{pmatrix} 0, & 1 \\ -1, & \delta_k \end{pmatrix}$ the substitution which converts ϕ_k into ϕ_{k+1}, $|\delta_k| = d_k$, ω_1 the principal root of ϕ_1, the absolute value of ω_1 may be expanded as a pure recurring chain-fraction in the form

$$|\omega_1| = \frac{1}{\underset{*}{d_1}} + \frac{1}{d_2} + \dots + \frac{1}{\underset{*}{d_{2m}}} + \dots.$$

In the same way, if ω_k is the principal root of ϕ_k,

$$|\omega_k| = \frac{1}{\underset{*}{d_k}} + \frac{1}{d_{k+1}} + \dots + \frac{1}{\underset{*}{d_{k-1}}} + \dots.$$

For example, let $\phi_1=(1,\ 3,\ -4)$; then the corresponding period contains ten forms (cf. Art. 68). The values of δ_k are

$$1,\ -1,\ 1,\ -1,\ 6,\ -1,\ 1,\ -1,\ 1,\ -6\,;$$

and hence

$$\omega_1=\sqrt{13}-3=\underset{*}{\frac{1}{1+}}\,\frac{1}{1+}\,\frac{1}{1+}\,\frac{1}{1+}\,\underset{*}{\frac{1}{6+}}\dots.$$

Here it will be observed that the period of ten forms gives rise to a recurring fraction with only five partial quotients in its period. The reason for this will appear later on.

73. It is now evident that the reduction of an indefinite form is precisely equivalent to the expansion of its principal root in the form of a recurrent fraction; in particular, we have found the necessary and sufficient conditions that a root of a quadratic equation should be expressible as a *pure* recurring fraction. Another curious point is that in the expansion of expressions such as $(b+\sqrt{D})/a$ only a limited number of distinct periods of partial quotients can occur; thus for $D=13$ there are only two, namely $(1,\ 1,\ 1,\ 1,\ 6)$ and (3). Here periods derived by cyclical permutation, such as $(1,\ 6,\ 1,\ 1,\ 1)$, are not considered to be distinct.

74. If $(a,\ b,\ -a')$ is a reduced form, so also is $(-a',\ b,\ a)$. These may be called *associated* forms. Two associated forms may occur either in different periods, or in the same period. In the first case, it is easily seen that each form of one period is associated with a corresponding form of the other; and the periods may be called associated. Suppose, on the other hand, that the forms occur in the same period. Then if $(-a',\ b',\ a'')$ is the form of the period next after $(a,\ b,\ -a')$, its associate $(a'',\ b',\ -a')$ is the form next before $(-a',\ b,\ a)$; and similarly, if $(-a',\ b',\ a'')$ is followed by $(a'',\ b'',\ -a''')$, $(-a''',\ b'',\ a'')$ will precede $(a'',\ b',\ -a')$. Proceeding in this way, forwards from $(a,\ b,\ -a')$ and backwards from $(-a',\ b,\ a)$, we come eventually to a pair of associated forms $(A,\ B,\ -A')$, $(-A',\ B,\ A)$ which are consecutive forms in the period. Since these are adjacent, $B+B\equiv 0 \pmod{A'}$, that is, $2B\equiv 0 \pmod{A'}$; $(-A',\ B,\ A)$ is therefore an ambiguous form (cf. Art. 62). In the same manner, by going forwards from $(-a',\ b,\ a)$ and backwards from $(a,\ b,\ -a')$, we arrive at a pair of associated forms which are adjacent; one of these is therefore ambiguous. Thus every period which is its own associate contains two ambiguous forms; and conversely, if a period contains one ambiguous form, it must be its own associate, and will contain a second ambiguous form. There cannot be more than two ambiguous forms in a period; for by proceeding forwards and backwards from an ambiguous form $(A, B, -A')$ and its predecessor $(-A', B, A)$, we obtain continually new pairs of associated forms $(a, b, -a')$, $(-a', b, a)$, and if either of these is ambiguous, it is adjacent to the other, and the period is completed.

75. If $(A, B, -A')$ is a reduced form, so also is $(-A, B, A')$. The principal roots of these forms are equal and opposite; hence the recurrent expansions of their absolute values coincide. It may happen that $(A, B, -A')$ and $(-A, B, A')$ belong to the same period; suppose that this is the case, and that the period contains $2m$ forms. Then if, with the notation of Art. 72, we put $(A, B, -A') = \phi_1$, it is easily seen that $(-A, B, A') = \phi_{m+1}$, and that $\delta_{m+1} = -\delta_1$, $\delta_{m+2} = -\delta_2, \ldots \delta_{2m} = -\delta_m$. Consequently

$$d_{m+1} = d_1,\ d_{m+2} = d_2, \ldots d_{2m} = d_m;$$

and the series of recurring partial quotients in the expansion of the principal root of $(A, B, -A')$ contains only half as many terms as there are forms in the period.

An example has already been given above (Art. 72) for $D = 13$. Here the forms $(1, 3, -4)$ and $(-1, 3, 4)$ belong to the same period of ten forms; and the periodic expansion of the absolute value of the principal root of either is $(0;\ \overset{*}{1}, 1, 1, 1, \overset{*}{6})$.

All the forms of a period of this kind may be arranged in pairs such as $(a, b, -a')$, $(-a, b, a')$, with equal and opposite principal roots.

If the forms $(a, b, -a')$, $(-a, b, a')$ are equivalent, and $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$ is a substitution transforming $(a, b, -a')$ into $(-a, b, a')$, then, ω being the principal root of the first form,

$$\omega = \frac{\alpha(-\omega) + \beta}{\gamma(-\omega) + \delta},$$

or

$$\gamma\omega^2 - (\alpha + \delta)\omega + \beta = 0.$$

Comparing this with $a\omega^2 + 2b\omega - a' = 0$, and proceeding exactly as in Art. 83 below, we have

$$\alpha = (t - bu)/\sigma, \quad \gamma = au/\sigma,$$
$$\beta = -a'u/\sigma, \qquad \delta = -(t + bu)/\sigma,$$

where $\sigma = dv\,(a,\ 2b,\ c)$, and $(t,\ u)$ is an integral solution of

$$t^2 - Du^2 = -\sigma^2.$$

Conversely, if this equation admits of integral solutions, the forms of any period for the determinant D and divisor σ may be arranged in pairs $(a,\ b,\ -a')$, $(-a,\ b,\ a')$. If the equation is solvable for $\sigma = 1$, it is so for $\sigma = 2$; in this case, both the properly and the improperly primitive periods have the special character in question. If the equation has integral solutions only for $\sigma = 2$, the property will belong only to the improperly primitive periods.

76. In order to complete the theory, it has to be shown that two equivalent reduced forms must belong to the same period. This is the most difficult part of the whole investigation, and requires the proof of some auxiliary propositions.

The notation $(\mu_0;\ \mu_1,\ \mu_2, \ldots)$ will be used to express the continued fraction

$$\mu_0 + \frac{1}{\mu_1 +}\,\frac{1}{\mu_2 +} \ldots,$$

and in the case of a recurrent fraction, the period will be indicated by asterisks: thus

$$(1;\ \overset{*}{2},\ 3,\ \overset{*}{4}) \text{ means } 1 + \frac{1}{2 +}\,\frac{1}{3 +}\,\frac{1}{4 +} \ldots,$$

and

$$(0;\ \overset{*}{3}) \text{ means } \frac{1}{3 +}\,\frac{1}{3 +} \ldots.$$

A continued fraction (with a finite or infinite number of partial quotients) is said to be *regular*, when it is of the form $(\pm\mu_0;\ \mu_1,\ \mu_2,\ \mu_3 \ldots)$, where all the quantities $\mu_1,\ \mu_2,\ \mu_3 \ldots$ are positive and not zero. When this is not the case, it is *irregular*.

77. *If a continued fraction contains only a limited number of negative or zero partial quotients, then it is possible, by a finite number of operations, to convert it into a regular continued fraction.*

Let μ_r be the last partial quotient which is not positive. There are the following cases to consider.

I. $\mu_r = 0$.

We have identically

$$a + \cfrac{1}{0 + \cfrac{1}{b + \cfrac{1}{x}}} = (a + b) + \frac{1}{x};$$

hence without altering the value of the continued fraction we may replace the four partial quotients

$$\mu_{r-1},\ 0,\ \mu_{r+1},\ \mu_{r+2}$$

by

$$\mu_{r-1}+\mu_{r+1},\ \mu_{r+2},$$

leaving all the rest as before.

II. $\mu_r = -n$, and $n > 1$.

We have identically

$$a + \cfrac{1}{-b+\cfrac{1}{x}} = a - \frac{x}{bx-1}$$

$$= a - 1 + \frac{(b-1)x-1}{bx-1}$$

$$= a - 1 + \cfrac{1}{1+\cfrac{x}{(b-1)x-1}}$$

$$= a - 1 + \cfrac{1}{1+\cfrac{1}{(b-2)+\cfrac{x-1}{x}}}$$

$$= a - 1 + \cfrac{1}{1+\cfrac{1}{(b-2)+\cfrac{1}{1+\cfrac{1}{(x-1)}}}}.$$

Hence we may replace

$$\mu_{r-1},\quad -n,\quad \mu_{r+1}$$

by

$$\mu_{r-1}-1,\quad 1,\quad n-2,\quad 1,\quad \mu_{r+1}-1.$$

Of these only the first can be negative. If either $n-2$ or $\mu_{r+1}-1$ is zero, we can apply the reduction of the previous case.

III. $\mu_r = -1$.

We have identically

$$a + \cfrac{1}{-1+\cfrac{1}{x}} = a - \frac{x}{x-1}$$

$$= a - 2 + \frac{x-2}{x-1}$$

$$= a - 2 + \cfrac{1}{1+\cfrac{1}{x-2}}.$$

Therefore

$$\mu_{r-1}, \quad -1, \quad \mu_{r+1}$$

may be replaced by

$$\mu_{r-1}-2, \quad 1, \quad \mu_{r+1}-2.$$

If $\mu_{r+1}=2$, the first reduction may be applied. If $\mu_{r+1}=1$, the preceding process fails: but we have

$$a+\cfrac{1}{-1+\cfrac{1}{1+\cfrac{1}{b+\cfrac{1}{x}}}}=a+\frac{(b+1)x+1}{-x}=a-b-2+\frac{x-1}{x}$$

$$=a-b-2+\cfrac{1}{1+\cfrac{1}{(x-1)}};$$

so that we may replace

$$\mu_{r-1}, \quad -1, \quad 1, \quad \mu_{r+2}, \quad \mu_{r+3}$$

by

$$\mu_{r-1}-\mu_{r+2}-2, \quad 1, \quad \mu_{r+3}-1.$$

If $\mu_{r+3}-1$ is zero, the first reduction can be made.

It will be seen that in every case the last irregularity is brought at least one place nearer to the beginning of the fraction. It is therefore possible, by repeated reductions, to bring it to the first place, and the fraction has then become regular.

Moreover each reduction either leaves the total number of partial quotients unaltered, or else increases or diminishes them by *two*. If the process be applied to an infinite continued fraction (that is, one with an infinite number of partial quotients), only a limited number of partial quotients will be affected, *and those which remain unaltered will occupy odd or even places in the regular expansion according as their places were odd or even originally.*

78. Another lemma which will be required is the following:—

If the quantities x, y are connected by the relation

$$y=\frac{\alpha x+\beta}{\gamma x+\delta},$$

where α, β, γ, δ are integers such that $\alpha\delta-\beta\gamma=1$, it is always possible to express y in the form

$$y=(\pm\mu;\ \mu_1,\ \mu_2,\ldots\mu_{2r},\ \pm\nu,\ x),$$

where $\mu_1, \mu_2, \ldots \mu_{2r}$ are all positive.

Let $\pm\mu$ be determined so that $\beta/\delta \mp \mu$ is a positive proper fraction: this proper fraction may be expanded into an ordinary continued fraction in the usual way, and if it happens that the number of partial quotients is odd, the last of them, μ_{2r-1} say, may be replaced by $(\mu_{2r-1}-1)+1/1$, and then we may write μ_{2r-1} for $\mu_{2r-1}-1$, and put $\mu_{2r}=1$. Thus in all cases

$$\frac{\beta}{\delta}=(\pm\mu\,;\ \mu_1,\ \mu_2,\ldots\mu_{2r}).$$

Suppose that α_1/γ_1 is the convergent immediately preceding β/δ; then

$$\alpha_1\delta-\gamma_1\beta=1=\alpha\delta-\gamma\beta,$$

and hence

$$\alpha=\alpha_1\pm\nu\beta,$$
$$\gamma=\gamma_1\pm\nu\delta,$$

where ν is some integer. It follows from this that

$$\alpha/\gamma=(\pm\mu\,;\ \mu_1,\ \mu_2,\ldots\mu_{2r},\ \pm\nu),$$

and that

$$y=\frac{\alpha x+\beta}{\gamma x+\delta}=(\pm\mu\,;\ \mu_1,\ \mu_2,\ldots\mu_{2r},\ \pm\nu,\ x).$$

Example 1. Suppose $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}=\begin{pmatrix}11, & -6\\ -9, & 5\end{pmatrix}$.

Here

$$-6/5=-2+4/5=(-2\,;\ 1,\ 4);$$
$$\alpha_1=-1,\qquad \gamma_1=1,$$
$$\alpha\ =11=-1+(-2)(-6),$$
$$\gamma\ =-9=1+(-2)(5),$$

and therefore

$$y=\frac{11x-6}{-9x+5}=(-2\,;\ 1,\ 4,\ -2,\ x).$$

Example 2.

$$\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}=\begin{pmatrix}30, & -67\\ -47, & 105\end{pmatrix},$$
$$\beta/\delta=(-1\,;\ 2,\ 1,\ 3,\ 4,\ 1,\ 1),$$
$$\alpha_1=-37,\qquad \gamma_1=58,$$
$$\alpha\ =\alpha_1+67,\quad \gamma\ =\gamma_1-105\,;$$

therefore $\nu=-1$, and

$$y=\frac{30x-67}{-47x+105}=(-1\,;\ 2,\ 1,\ 3,\ 4,\ 1,\ 1,\ -1,\ x).$$

79. We are now able to prove that two properly equivalent reduced forms must belong to the same period. Let the reduced forms be $\phi=(a, b, -c)$ and $\phi'=(a', b', -c')$: we may suppose that a, a' are both positive, because if, for instance, a were negative we could take instead of ϕ one of the two adjacent forms of the same period.

Let ω, ω' be the principal roots of ϕ and ϕ'; these will be positive proper fractions. If $\phi' \backsim \phi$, there will be a proper substitution $\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}$ which will transform ϕ' into ϕ, and therefore

$$\omega' = \frac{\alpha\omega + \beta}{\gamma\omega + \delta}.$$

By the lemma just proved, we can express ω' in the form

$$\begin{aligned}\omega' &= (\pm\mu;\ \mu_1,\ \mu_2, \ldots \mu_{2r},\ \pm\nu,\ \omega) \\ &= (\pm\mu;\ \mu_1,\ \mu_2, \ldots \mu_{2r},\ (\pm\nu + d_1),\ \overset{*}{d}_2,\ d_3, \ldots d_{2m},\ \overset{*}{d}_1),\end{aligned}$$

if $(0;\ \overset{*}{d}_1,\ d_2, \ldots \overset{*}{d}_{2m})$ is the recurrent expansion of ω.

If $d_1 \pm \nu$ happens to be negative, the expression for ω' can be reduced to a regular expansion, so that we may write in every case

$$\omega' = (\pm\mu';\ l_1,\ l_2,\ l_3, \ldots),$$

where l_1, l_2, $l_3, \ldots$ are all positive.

Now ω' is a positive proper fraction; therefore $\mu'=0$. Again, ω' can be expressed in one way only as a pure recurring fraction; hence l_1, l_2, $l_3 \ldots$ must form the recurring period of ω'. But in the reduction of the first expression for ω' into a regular form, only a finite number of partial quotients after $\pm\nu$ are affected. Therefore the series $(l_1, l_2, l_3 \ldots)$ only differs from $(d_1, d_2, d_3 \ldots)$ by beginning at a different place; in other words, the period of partial quotients in the expansion of ω' is only a cyclical permutation of the period belonging to ω, and moreover a permutation equivalent to an *even* number of transpositions (cf. Art. 77 above). Therefore the forms ϕ and ϕ' belong to the same period.

The following example will illustrate this theorem, as well as the reduction of irregular continued fractions.

The form $\phi'=(6, 1, -7)$ is transformed into $\phi=(9, 5, -2)$ by the substitution $\begin{pmatrix}29, & -5 \\ -23, & 4\end{pmatrix}$.

Now $$-\frac{5}{4} = (-2;\ 1,\ 3),$$

and $$\omega' = \frac{29\omega - 5}{-23\omega + 4} = (-2;\ 1,\ 3,\ -6,\ \omega);$$

or, since
$$\begin{aligned}\omega &= (0\,;\ \overset{*}{5},\ 1,\ 3,\ 1,\ 1,\ \overset{*}{12}),\\ \omega' &= (-2\,;\ 1,\ 3,\ -1,\ \overset{*}{1},\ 3,\ 1,\ 1,\ldots)\\ &= (-2\,;\ 1,\ -2,\ 1,\ 0,\ \overset{*}{1},\ 12,\ldots)\\ &= (-2\,;\ 1,\ -2,\ 2,\ \overset{*}{12},\ldots)\\ &= (-2\,;\ 0,\ 1,\ 0,\ \overset{*}{1},\ 1,\ 12,\ldots)\\ &= (-2\,;\ 0,\ 2,\ \overset{*}{1},\ 12,\ldots)\\ &= (0\,;\ \overset{*}{1},\ 12,\ 5,\ 1,\ 3,\ \overset{*}{1}),\end{aligned}$$
the period of which is derived from that of ω by cyclical permutation, each element being removed four places backwards.

80. In order to discover whether two given forms, f, f', of the same determinant, are equivalent, we find, by the process of Art. 69, two reduced forms ϕ, ϕ' equivalent to f, f' respectively. The necessary and sufficient condition for the equivalence of f and f' is that ϕ and ϕ' should belong to the same period of reduced forms. Suppose that this is so, and that $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$, $\begin{pmatrix}\lambda, & \mu\\ \nu, & \rho\end{pmatrix}$, $\begin{pmatrix}\alpha', & \beta'\\ \gamma', & \delta'\end{pmatrix}$ respectively transform f into ϕ, ϕ into ϕ', and f' into ϕ'. Then the substitution
$$\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}\begin{pmatrix}\lambda, & \mu\\ \nu, & \rho\end{pmatrix}\begin{pmatrix}\delta', & -\beta'\\ -\gamma', & \alpha'\end{pmatrix}$$
will transform f into f'.

Example. $D = 43$,
$$f = (53,\ 72,\ 97),\quad f' = (-19,\ 47,\ -114).$$

We have
$$\begin{aligned}(53,\ 72,\ 97) &\sim (97,\ 25,\ 6)\\ &\sim (6,\ 5,\ -3)\\ &\sim (-3,\ 4,\ 9) = \phi\end{aligned}$$
and
$$\begin{aligned}(-19,\ 47,\ -114) &\sim (-114,\ 67,\ -39)\\ &\sim (-39,\ 11,\ -2)\\ &\sim (-2,\ 5,\ 9) = \phi'.\end{aligned}$$

The period of $(-3,\ 4,\ 9)$ is
$$(-3,\ 4,\ 9),\quad (9,\ 5,\ -2),\quad (-2,\ 5,\ 9),\ \text{etc.},$$
hence $\phi \sim \phi'$, and therefore $f \sim f'$.

Again f is transformed into ϕ by the substitution

$$\begin{pmatrix} 0, & 1 \\ -1, & -1 \end{pmatrix}\begin{pmatrix} 0, & 1 \\ -1, & -5 \end{pmatrix}\begin{pmatrix} 0, & 1 \\ -1, & 3 \end{pmatrix}=\begin{pmatrix} 5, & -16 \\ -4, & 13 \end{pmatrix};$$

ϕ into ϕ' by

$$\begin{pmatrix} 0, & 1 \\ -1, & -1 \end{pmatrix}\begin{pmatrix} 0, & 1 \\ -1, & 5 \end{pmatrix}=\begin{pmatrix} -1, & 5 \\ 1, & -6 \end{pmatrix};$$

f' into ϕ' by

$$\begin{pmatrix} 0, & 1 \\ -1, & 1 \end{pmatrix}\begin{pmatrix} 0, & 1 \\ -1, & 2 \end{pmatrix}\begin{pmatrix} 0, & 1 \\ -1, & 8 \end{pmatrix}=\begin{pmatrix} -2, & 15 \\ -1, & 7 \end{pmatrix}.$$

Therefore f is transformed into f' by the substitution

$$\begin{pmatrix} 5, & -16 \\ -4, & 13 \end{pmatrix}\begin{pmatrix} -1, & 5 \\ 1, & -6 \end{pmatrix}\begin{pmatrix} 7, & -15 \\ 1, & -2 \end{pmatrix}=\begin{pmatrix} -26, & 73 \\ 21, & -59 \end{pmatrix}.$$

Simplest Representative Forms.

81. The most important result which has been obtained is that both for definite and for indefinite forms the number of classes for a given determinant is finite. To assign, *a priori*, the number of classes, without constructing a system of reduced forms, is a fundamental problem of which the interest is equalled by its difficulty, and all the solutions hitherto obtained depend upon the most abstruse analytical methods. An account of these investigations will be given later on; meanwhile, it may be observed that, from this point of view, a system of reduced forms is merely a finite number of forms such that every form of the determinant considered is properly equivalent to at least one of them. Consequently the definition of a reduced form is to a certain extent arbitrary; and in like manner with regard to the choice of a complete system of representative forms. We may, in fact, take as the representative of a class any form which is contained in it; however, it is convenient to fix upon a set of 'simplest representative forms,' which are defined as follows.

When D is negative, there cannot be more than two reduced forms in any class. When there is only one, that is chosen for the representative; when there are two, in which case they are opposite, that one is taken of which the middle coefficient is positive (cf. Art. 66).

When D is positive, the period of reduced forms for any class will contain either two ambiguous forms or none (Art. 74). In the former case, let the ambiguous forms be (a, b, c), (a', b', c'). We can find two other forms equivalent to these, of which the middle coefficients shall be the absolutely least residues of b, b' to the moduli a, a' respectively. If in one only of these new forms the middle coefficient be zero, that form is chosen; if neither or both of the middle coefficients be zero, that form is taken of which the first coefficient is numerically least. If the first coefficients are numerically equal and of opposite signs, we choose the form of which the first coefficient is positive. When the period contains no ambiguous form, we choose that form (a, b, c) of which the first coefficient has the least numerical value (if there are two such coefficients, only differing in sign, we take the form of which the first coefficient is positive); then, as before, we deduce from this the form (a, b', c'), where b' is the absolutely least residue of b (mod a), and take this for the representative form.

Thus for $D = 58$, there is a period $(2, 6, -11)$, $(-11, 5, 3)$, $(3, 7, -3)$, $(-3, 5, 11)$, $(11, 6, -2)$, $(-2, 6, 11)$, etc. The ambiguous forms are $(2, 6, -11)$ and $(-2, 6, 11)$, from the former of which we derive the representative form $(2, 0, -29)$. Or again for $D = 99$ we have a period $(5, 8, -7)$, $(-7, 6, 9)$, $(9, 3, -10)$, $(-10, 7, 5)$; here we choose $(5, 8, -7)$ and deduce from it the representative form $(5, -2, -19)$.

Automorphic Substitutions.

82. Suppose that it has been discovered, by the methods already explained, that two forms f and f' are equivalent. The process by which the equivalence is established also furnishes a proper substitution by which f is transformed into f'. The question arises; is this the only substitution by which the transformation can be effected? and, if not, how can we find all the substitutions which transform f into f'?

This problem may be at once reduced to that of finding all the substitutions which transform f into itself. It is clear that if R is any substitution which transforms f into itself, and S any substitution which transforms f into f', then the substitution RS will also transform f into f'. Moreover, if S_1, S_2 are any two different substitutions which transform f into f', the substitution $S_2S_1^{-1}$ will transform f into itself. Hence, putting $S_2S_1^{-1} = R$, we have $S_2 = RS_1$: so that all the substitutions which convert f into f'

may be obtained by compounding any one of them, such as S_1, with all the substitutions which leave f unaltered.

A proper substitution R which transforms f into itself is called an *automorphic substitution* (relatively to f), or simply an *automorph* of f.

83. Let $f = (a, b, c)$ be a primitive form of determinant D, and let ω be its principal root; then if $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ be an automorph,

$$\omega = \frac{\alpha\omega + \beta}{\gamma\omega + \delta}$$

or

$$\gamma\omega^2 + (\delta - \alpha)\,\omega - \beta = 0.$$

Comparing this with $a\omega^2 + 2b\omega + c = 0$, it follows that

$$\gamma = au/\sigma,$$
$$\delta - \alpha = 2bu/\sigma,$$
$$\beta = -\,cu/\sigma,$$

where u is an integer, and $\sigma = dv\,(a,\ 2b,\ c)$: that is, $\sigma = 1$ or 2 according as f is properly or improperly primitive. Since

$$(\delta + \alpha) + (\delta - \alpha) = 2\delta,$$

an even integer, we may evidently put $\delta + \alpha = 2t/\sigma$, where t is an integer. Thus

$$\left.\begin{aligned}\alpha &= (t - bu)/\sigma, & \beta &= -\,cu/\sigma,\\ \gamma &= au/\sigma, & \delta &= (t + bu)/\sigma\end{aligned}\right\}\ \ldots\ldots\ldots\ldots\ \text{(i)},$$

and substituting in $\alpha\delta - \beta\gamma = 1$, we obtain

$$t^2 - Du^2 = \sigma^2\ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ \text{(ii)}.$$

Thus all the automorphs $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ are expressible in the form given by (i), where t, u are integers which satisfy the indeterminate equation (ii).

Conversely, if t, u are any integers such that $t^2 - Du^2 = \sigma^2$, the values of α, β, γ, δ given by (i) will all be integral, and $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ will be an automorph. It may easily be verified that $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ is an *algebraical* automorph; so that all we have to do is to prove that α, β, γ, δ are integers. This is obvious when $\sigma = 1$; if $\sigma = 2$, $D \equiv 1 \pmod 4$, and the equation $t^2 - Du^2 = 4$ shows that t, u are both odd or both even. Also b is odd, otherwise f would not be primitive;

therefore $t-bu$ and $t+bu$ are both even, and consequently α, δ are integers. Finally, a, c are both even, and therefore β, γ are integers.

84. The equation (ii), although originally proposed for solution by Fermat, is usually known as the Pellian equation. Its character, from our present standpoint, is essentially different, according as D is positive or negative.

First, let $D=-\Delta$, a negative integer; then, in general, the only real integral solutions of $t^2+\Delta u^2=\sigma^2$ are $t=\pm\sigma$, $u=0$.

If $\sigma=1$, $\Delta=1$, they are $t=\pm 1$, $u=0$, and $t=0$, $u=\pm 1$.

If $\sigma=2$, $\Delta=3$, they are $t=\pm 2$, $u=0$, and $t=\pm 1$, $u=\pm 1$.

In general, therefore, there are only two solutions; the only exceptional cases (for primitive forms) being $\Delta=1$, $\sigma=1$, when there are four solutions, and $\Delta=3$, $\sigma=2$, for which there are six. Since the two solutions (t, u) $(-t, -u)$ lead to the same substitution, there is in general only one automorph, the identical substitution; for the exceptional cases we have two and three automorphs respectively. Thus the form (1, 0, 1) has the automorphs $\begin{pmatrix}1, & 0\\ 0, & 1\end{pmatrix}$ and $\begin{pmatrix}0, & -1\\ 1, & 0\end{pmatrix}$: while (2, 1, 2) has

$$\begin{pmatrix}1, & 0\\ 0, & 1\end{pmatrix}, \quad \begin{pmatrix}1, & 1\\ -1, & 0\end{pmatrix}, \quad \begin{pmatrix}0, & -1\\ 1, & 1\end{pmatrix}.$$

85. On the other hand, if D is positive, the Pellian equation admits of an infinite number of solutions. It can be shown, in the first place, that there is at least one solution distinct from $t=\pm\sigma$, $u=0$. For suppose (a, b, c) is a primitive reduced form of determinant D for which a is positive, and $dv\,(a, 2b, c)=\sigma$. Let its principal root be expanded into the recurrent fraction

$$\omega=(0;\ \overset{*}{d}_1, d_2, \ldots \overset{*}{d}_{2m}),$$

and suppose that p_{2m-1}/q_{2m-1}, p_{2m}/q_{2m} are the $(2m-1)$th and $2m$th convergents. Then since $\omega=(0;\ d_1, d_2, \ldots d_{2m-1}, d_{2m}+\omega)$, it follows that

$$\omega=\frac{p_{2m-1}\,\omega+p_{2m}}{q_{2m-1}\,\omega+q_{2m}},$$

hence $\begin{pmatrix}p_{2m-1}, & p_{2m}\\ q_{2m-1}, & q_{2m}\end{pmatrix}$ is an automorph, and therefore if we put

$$p_{2m-1}=(t-bu)/\sigma, \qquad p_{2m}=-cu/\sigma,$$
$$q_{2m-1}=au/\sigma, \qquad q_{2m}=(t+bu)/\sigma,$$

t, u will be positive integers such that $t^2-Du^2=\sigma^2$.

For instance, if $D=17$, we may take the reduced form $(2, 3, -4)$, for which $\sigma=2$. The expansion of its principal root is

$$(0;\ \overset{*}{1}, 1, 3, 1, 1, \overset{*}{3}),$$

whence $$p_5=9=\tfrac{1}{2}(t-3u), \quad q_5=16=u,$$

so that $$t=66, \quad u=16.$$

Excluding the case for which $t=\sigma$, $u=0$, there will be one positive integral solution of $t^2-Du^2=\sigma^2$ for which t, u have the smallest possible values. This will be denoted by (T, U) and called the fundamental solution.

If n is a positive integer, the expression $(T+U\sqrt{D})^n$ may be reduced to the form $P+Q\sqrt{D}$, where P, Q are integers, so that if we write

$$\left(\frac{T+U\sqrt{D}}{\sigma}\right)^n=\frac{T_n+U_n\sqrt{D}}{\sigma},$$

T_n, U_n will be rational. Moreover since $\sqrt{D}$ is irrational, we shall have

$$\left(\frac{T-U\sqrt{D}}{\sigma}\right)^n=\frac{T_n-U_n\sqrt{D}}{\sigma},$$

and hence, by multiplication,

$$\frac{T_n^2-DU_n^2}{\sigma^2}=\left(\frac{T^2-DU^2}{\sigma^2}\right)^n=1.$$

Therefore (T_n, U_n) is a rational solution of $t^2-Du^2=\sigma^2$. It may be shown that T_n, U_n are integers. This is evidently the case when $\sigma=1$; if $\sigma=2$, it may be proved by induction as follows. Suppose the theorem true up to (T_n, U_n); then since $D\equiv 1 \pmod 4$, the equation $T_n^2-DU_n^2=4$ shows that T_n, U_n as well as T, U are either both even or both odd. Now

$$\frac{T_{n+1}+U_{n+1}\sqrt{D}}{2}=\frac{T+U\sqrt{D}}{2}\cdot\frac{T_n+U_n\sqrt{D}}{2}$$
$$=\tfrac{1}{2}\left\{\frac{TT_n+DUU_n}{2}+\frac{T_nU+TU_n}{2}\sqrt{D}\right\};$$

hence $$T_{n+1}=\tfrac{1}{2}(TT_n+DUU_n)$$

and $$U_{n+1}=\tfrac{1}{2}(T_nU+TU_n)$$

are both integral, and since they satisfy $T^2_{n+1}-DU^2_{n+1}=4$, they are both odd or both even. The theorem being true for $n=1$, it is true universally.

86. Every positive integral solution is of the form (T_n, U_n) where

$$\frac{T_n + U_n \sqrt{D}}{\sigma} = \left(\frac{T + U\sqrt{D}}{\sigma}\right)^n,$$

and n is a positive integer.

For suppose, if possible, that (t, u) is any other positive solution. Then $t + u\sqrt{D} > T + U\sqrt{D}$, and since $T + U\sqrt{D} > \sigma$, there will be an integer n such that

$$\left(\frac{T + U\sqrt{D}}{\sigma}\right)^n < \frac{t + u\sqrt{D}}{\sigma} < \left(\frac{T + U\sqrt{D}}{\sigma}\right)^{n+1}.$$

Multiplying by $\left(\frac{T - U\sqrt{D}}{\sigma}\right)^n = \frac{T_n - U_n\sqrt{D}}{\sigma}$, which is positive, we obtain

$$1 < \frac{t' + u'\sqrt{D}}{\sigma} < \frac{T + U\sqrt{D}}{\sigma},$$

where
$$t' = \frac{tT_n - DuU_n}{\sigma},$$

$$u' = \frac{T_n u - U_n t}{\sigma}.$$

As in last article, it can be proved that whether $\sigma = 1$ or $\sigma = 2$, t', u' are integers. Moreover

$$t'^2 - Du'^2 = \frac{1}{\sigma^2}(t^2 - Du^2)(T^2 - DU^2) = \sigma^2;$$

and this, combined with $t' + u'\sqrt{D} > \sigma$, gives $0 < t' - u'\sqrt{D} < \sigma$, so that t', u' are *positive* integers.

Again, $$t' + u'\sqrt{D} < T + U\sqrt{D},$$

and $$(t' + u'\sqrt{D})(t' - u'\sqrt{D}) = \sigma^2 = (T + U\sqrt{D})(T - U\sqrt{D});$$

therefore $$t' - u'\sqrt{D} > T - U\sqrt{D}:$$

consequently

$$(t' + u'\sqrt{D}) - (t' - u'\sqrt{D}) < (T + U\sqrt{D}) - (T - U\sqrt{D}),$$

and hence $u' < U$. Therefore also $t' < T$; so that (t', u') is a positive integral solution of $t^2 - Du^2 = \sigma^2$, for which the values of t, u are less than T, U. But this contradicts the hypothesis that (T, U) is the fundamental solution; therefore there are no positive solutions except those given by $\frac{T_n + U_n\sqrt{D}}{\sigma} = \left(\frac{T + U\sqrt{D}}{\sigma}\right)^n$.

All the integral solutions are given by ($\pm T_n$, $\pm U_n$), where the ambiguities are independent.

By giving to n the values 2, 3, 4..., we obtain an infinite number of positive solutions (T_n, U_n) which are all different, since evidently $T_{n+1} > T_n$, and $U_{n+1} > U_n$.

We may, if we like, assign negative values to n, and put

$$\frac{T_{-n}+U_{-n}\sqrt{D}}{\sigma}=\left(\frac{T+U\sqrt{D}}{\sigma}\right)^{-n};$$

since $$\left(\frac{T+U\sqrt{D}}{\sigma}\right)^{-1}=\frac{T-U\sqrt{D}}{\sigma},$$

we have $$\frac{T_{-n}+U_{-n}\sqrt{D}}{\sigma}=\frac{T_n-U_n\sqrt{D}}{\sigma},$$

so that $$T_{-n}=T_n,\ U_{-n}=-U_n.$$

If, in the notation of the hyperbolic functions, we put

$$\phi=\cosh^{-1}(T/\sigma)=\sinh^{-1}(U\sqrt{D}/\sigma),$$

we shall have $T_n=\sigma\cosh n\phi$, $U_n\sqrt{D}=\sigma\sinh n\phi$.

The convenience of this is that the known formulæ of the hyperbolic functions may be used to express the relations between the different values (T_n, U_n). Thus from the formulæ

$$\cosh 2\phi=2\cosh^2\phi-1,\quad \sinh 2\phi=2\sinh\phi\cosh\phi,$$

we deduce $\sigma T_{2n}=2T_n^2-\sigma^2$, $\sigma U_{2n}=2T_nU_n$; and so in other cases. It may be specially observed that

$$T_{n+1}=\frac{2T}{\sigma}\,.\,T_n-T_{n-1},$$

$$U_{n+1}=\frac{2T}{\sigma}\,.\,U_n-U_{n-1};$$

these formulæ are very convenient for the calculation of the successive values of T_n, U_n.

87. Let $\sigma=1$ for the moment, and for the sake of uniformity write $T_0=1$, $U_0=0$, $T_1=T$, $U_1=U$. If p is an odd prime, we have

$$\begin{aligned}T_p+U_p\sqrt{D}&=(T_1+U_1\sqrt{D})^p\\&\equiv T_1^p+U_1^pD^{\frac{1}{2}p}\ (\text{mod } p)\\&\equiv T_1+D^{\frac{1}{2}(p-1)}U_1\sqrt{D}.\end{aligned}$$

Hence $$T_p\equiv T_1,$$
$$U_p\equiv(D\,|\,p)\,U_1,$$

if we adopt the convention that $(D \mid p) = 0$ when p is a factor of D. If we write ϵ for $(D \mid p)$, we have $T_p \equiv T_\epsilon$, $U_p \equiv U_\epsilon$, supposing that p does not divide D. Also

$$\begin{aligned} T_{p+1} &= T_1 T_p + DU_1 U_p \\ &\equiv T_1 T_\epsilon + DU_1 U_\epsilon \equiv U_{1+\epsilon}, \\ U_{p+1} &= T_p U_1 + T_1 U_p \equiv U_{1+\epsilon}, \end{aligned}$$

and hence in general

$$T_{np+h} \equiv T_{n\epsilon+h},\ U_{np+h} \equiv U_{n\epsilon+h}.$$

We conclude, therefore, that the least positive residues of (T_n, U_n) with respect to p form a recurrent series, the number of terms in each period being a factor of $p - (D \mid p)$.

If p divides D, $T_1 \equiv \pm 1 \pmod p$, and the same reasoning shows that the residues recur with a period of p or $2p$ terms, according as $T \equiv 1$ or $-1 \pmod p$.

With respect to the modulus 2, the system of residues may be $(1, 0)$, or $(0, 1)$, $(1, 0)$, or $(1, 1)$, $(1, 0)$.

It is easy to see that a similar recurrence will exist if the residues are taken with respect to a composite modulus m. Thus if (T', U') is the least positive solution of $t^2 - m^2Du^2 = 0$, (T', mU') is a solution of $t^2 - Du^2 = 1$ for which $u = mU' \equiv 0 \pmod m$, and it is the first of the kind which occurs. Putting $T' = T_\lambda$, $mU' = U_\lambda$, we have $T_\lambda^2 \equiv 1 \pmod m$; if $T_\lambda \equiv 1 \pmod m$, the period contains λ terms; if not, $T_{2\lambda} \equiv 2T_\lambda^2 - 1 \equiv 1 \pmod m$, $U_{2\lambda} \equiv 2T_\lambda U_\lambda \equiv 0 \pmod m$, and the period contains 2λ terms.

It does not seem easy to assign the number of terms in the period of residues when m, D are given. By arguments similar to those employed in Chap. I. it is possible to prove the following theorem, which may serve as an exercise for the reader.

Suppose that m contains at least one odd prime factor which does not divide D: then if $p, q, r \ldots$ are the different odd primes which divide m but not D, and if μ is the L.C.M. of $m/pqr \ldots$, $p - (D \mid p)$, $q - (D \mid q)$, etc., the number of terms in a period will certainly divide μ. *A fortiori* it will divide

$$\frac{m}{2^{a-1}} \Pi \left(1 - \frac{1}{p}(D \mid p)\right),$$

where the product applies to all odd primes which divide m but not D, and a is the number of such primes.

If every prime factor of m divides D, all that can be concluded is that the number of terms in a period divides $2m$.

Examples. $D=11$, $T_1=10$, $U_1=3$, $m=75$. Here, since $(11\,|\,5)=+1$, and $(11\,|\,3)=-1$, μ is the L.C.M. of 5, 4, 4, that is, 20. The period of residues does in fact contain 20 terms, viz.

$$\begin{array}{llll}(10,\ 3), & (49,\ 60), & (70,\ 72), & (1,\ 30),\\ (25,\ 3), & (49,\ 30), & (55,\ 72), & (1,\ 60),\\ (40,\ 3), & (49,\ \ 0), & (40,\ 72), & (1,\ 15),\\ (55,\ 3), & (49,\ 45), & (25,\ 72), & (1,\ 45),\\ (70,\ 3), & (49,\ 15), & (10,\ 72), & (1,\ \ 0).\end{array}$$

If $m=11$, there are 22 terms in the period; namely (10, 3), (1, 5), (10, 9), (1, 10), etc.

The number of terms in the period is often less than μ: thus for $D=11$, $m=9$, μ is 12, but the period is (1, 3), (1, 6), (1, 0).

88. The complete system of automorphs for a primitive form (a, b, c) is given by

$$\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}=\begin{pmatrix}(T_n-bU_n)/\sigma, & -cU_n/\sigma\\ aU_n/\sigma, & (T_n+bU_n)/\sigma\end{pmatrix},$$

where T_n, U_n have the meaning already defined; except that in this formula they may be taken positively or negatively. If, as we have tacitly done hitherto, we consider $\begin{pmatrix}-\alpha, & -\beta\\ -\gamma, & -\delta\end{pmatrix}$ the same as $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$, it is sufficient to give to n all positive and negative integral values and take T_n, U_n with the signs appropriate to them in each case, according to Art. 86.

With this convention, let the substitution above written be denoted by S_n. Then it is easily verified that if m, n are any integers,

$$S_m\,.\,S_n=S_{m+n}=S_n\,.\,S_m,$$

and hence, if S denote

$$\begin{pmatrix}(T-bU)/\sigma, & -cU/\sigma\\ aU/\sigma, & (T+bU)/\sigma\end{pmatrix},$$

$$S_n=S^n;$$

therefore all the automorphic substitutions may be expressed as powers of the fundamental substitution S.

It has already been shown (Art. 85) that from the period of a reduced form $(a,\ b,\ -a')$ an automorphic substitution may be derived. It is not difficult to prove that this is the fundamental automorph. For simplicity, suppose that a is positive, and let the derived automorph be

$$S' = \begin{pmatrix} (t' - bu')/\sigma, & a'u'/\sigma \\ au'/\sigma, & (t' + bu')/\sigma \end{pmatrix},$$

where t' is positive.

Since $t'^2 - b^2u'^2 = aa'u'^2 + \sigma^2$, $t' - bu'$ and $t' + bu'$ are positive. If S' is not the fundamental automorph, it must be a power of it, say S^k. It follows from this that if $au'/(t' + bu')$ be expanded into a continued fraction, the series of partial quotients will consist of those belonging to the expansion of $aU/(T + bU)$, repeated k times. But in the series $d_1, d_2, \ldots d_{2m}$ derived from the period of reduced forms, such a repetition can only occur once. The only possible supposition therefore is that $S' = S^2$, and that S is derived from the partial quotients $d_1, d_2, \ldots d_m$. But these partial quotients lead to a solution, not of $t^2 - Du^2 = \sigma^2$, but of

$$t^2 - Du^2 = -\sigma^2$$

(cf. Art. 75). Therefore S' is the fundamental automorph.

The automorphs of a derived form are the same as those of the primitive from which it is derived.

89. If $R = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$ is any substitution which converts (a, b, c) into the equivalent form (a', b', c'), and if S is the fundamental automorph of (a, b, c), then all the substitutions which convert (a, b, c) into (a', b', c') are given by

$$\begin{pmatrix} \alpha_n, & \beta_n \\ \gamma_n, & \delta_n \end{pmatrix} = S^n R,$$

where n is any positive or negative integer.

The values of $\alpha_n, \beta_n, \gamma_n, \delta_n$ are

$$\alpha_n = \{\alpha T_n - (b\alpha + c\gamma) U_n\}/\sigma, \quad \beta_n = \{\beta T_n - (b\beta + c\delta) U_n\}/\sigma,$$
$$\gamma_n = \{\gamma T_n + (a\alpha + b\gamma) U_n\}/\sigma, \quad \delta_n = \{\delta T_n + (a\beta + b\delta) U_n\}/\sigma.$$

The relations between the original and the new variables may also be expressed by writing

$$ax + (b + \sqrt{D})y = \frac{T_n + U_n\sqrt{D}}{\sigma}\{a(\alpha x' + \beta y') + (b + \sqrt{D})(\gamma x' + \delta y')\};$$

and similarly, the automorphs of (a, b, c) may be derived from

$$ax + (b + \sqrt{D})y = \frac{T_n + U_n\sqrt{D}}{\sigma}\{ax' + (b + \sqrt{D})y'\}.$$

Representation of Numbers resumed.

90. It has already been shown (Art. 59) that if a number m is properly representable by a form of determinant D, D must be a quadratic residue of m. Further, if n is any root of the congruence

$$n^2 \equiv D \pmod{m},$$

and we put $(n^2 - D)/m = l$, then the form (m, n, l) is of determinant D, and any primitive representation $m = a\alpha^2 + 2b\alpha\gamma + c\gamma^2$ by the form (a, b, c) of determinant D leads to a proper substitution $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ by which (a, b, c) is transformed into (m, n, l).

In order, therefore, to determine whether m can be represented by a given form (a, b, c) we first find all the solutions of $n^2 \equiv D \pmod{m}$; taking any one of these, say n, we examine whether the forms (a, b, c), (m, n, l) are properly equivalent. If they are, the process by which we discover the equivalence enables us to form a substitution $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ which converts (a, b, c) into (m, n, l), and then $x = \alpha$, $y = \gamma$ gives a primitive representation of m by the form (a, b, c). This representation, moreover, appertains to the particular solution (n) of the congruence $n^2 \equiv D \pmod{m}$.

If, for a given value of $n \pmod{m}$, a particular solution is $x = \alpha$, $y = \gamma$, then (by Art. 89) the most general solution appertaining to this root of the congruence is

$$x = \frac{\alpha t - (b\alpha + c\gamma)\,u}{\sigma}, \qquad y = \frac{\gamma t + (a\alpha + b\gamma)\,u}{\sigma},$$

where $\sigma = dv\,(a, 2b, c)$ and (t, u) is any integral solution of

$$t^2 - Du^2 = \sigma^2.$$

By giving to t, u all suitable values we thus obtain a group of representations; there will be a finite or infinite number of representations in the group according as D is negative or positive.

The maximum number of distinct groups will be equal to the number of the solutions of the congruence $n^2 \equiv D \pmod{m}$.

91. Some illustrations of the general theory will now be given.

Example 1. Suppose $D = -1$. There is only one positive class for this determinant: its representative is $(1, 0, 1)$. Let m be a positive integer such that m or $\frac{1}{2}m$ is odd; then the congruence $n^2 \equiv -1 \pmod{m}$ is solvable if every odd prime which divides m is of the form $4n+1$. If this condition is satisfied, there will be a form (m, n, l) of determinant -1, and this must be equivalent to the reduced form $(1, 0, 1)$; therefore m can be expressed as the sum of two squares.

A special case of this is the famous theorem first enunciated by Fermat (*Observations on Diophantus*, No. VII.);

Every odd prime of the form $4n+1$ *can be expressed in one way, and one way only, as the sum of two squares.*

For if $p = 4n+1$ be a prime the congruence $n^2 \equiv -1 \pmod{p}$ has two solutions, each of which (Art. 84) corresponds to four representations, so that there are eight representations altogether: but if $x = t$, $y = u$ be any one of these, we get exactly eight by putting $x = \pm t$, $y = \pm u$, or $x = \pm u$, $y = \pm t$, so that if we neglect the order of the terms, p is expressed in one way only in the form

$$p = t^2 + u^2.$$

For instance, let $p = 89$. The roots of $n^2 \equiv -1 \pmod{89}$ are $n \equiv \pm 34$; taking the upper sign, and applying the usual process of reduction, we have

$$(89, 34, 13) \backsim (13, 5, 2) \backsim (2, 1, 1) \backsim (1, 0, 1).$$

Hence we derive the substitution

$$\begin{pmatrix} 0, & 1 \\ -1, & -3 \end{pmatrix} \begin{pmatrix} 0, & 1 \\ -1, & -3 \end{pmatrix} \begin{pmatrix} 0, & 1 \\ -1, & -1 \end{pmatrix} = \begin{pmatrix} +3, & +2 \\ -8, & -5 \end{pmatrix},$$

which converts $(89, 34, 13)$ into $(1, 0, 1)$; and the second form is converted into the first by the inverse substitution $\begin{pmatrix} -5, & -2 \\ +8, & +3 \end{pmatrix}$. This gives the representation $89 = (-5)^2 + (+8)^2$. If we start with $(89, -34, 13)$, we obtain in a similar way

$$89 = (+8)^2 + (-5)^2 = 64 + 25$$

as before.

Example 2. *To find all the representations of* $85 = 5 \,.\, 17$ *as the sum of two squares.*

The roots of $n^2 \equiv -1 \pmod{85}$ are $n \equiv \pm 13, \pm 38$. The forms $(85, 13, 2)$, $(85, 38, 17)$ are converted into $(1, 0, 1)$ by the substitutions $\begin{pmatrix} -1, & -1 \\ +7, & +6 \end{pmatrix}$ and $\begin{pmatrix} -1, & +4 \\ +2, & -9 \end{pmatrix}$ respectively; and hence

$$85 = 49 + 36 = 4 + 81.$$

The forms $(85, -13, 2)$ and $(85, -38, 17)$ lead to the same results.

Example 3. *To find all the representations, primitive and derived, of* 81 *in the form* $3x^2 + 2xy - 12y^2$.

For the primitive representations we solve $n^2 \equiv 37 \pmod{81}$, whence $n \equiv \pm 19 \pmod{81}$. Then by successive reductions we find

$$\begin{aligned}(81, 19, 4) \backsim (4, 5, -3) \backsim (-3, 4, 7) \backsim (7, 3, -4)& \\ \backsim (-4, 5, 3) \backsim (3, 4, -7)& \\ \backsim (\ 3, 1, -12).&\end{aligned}$$

From this is derived the substitution $\begin{pmatrix} -163, & -26 \\ +\ 69, & +11 \end{pmatrix}$ which converts $(3, 1, -12)$ into $(81, 19, 4)$; and the corresponding representation is $x = -163$, $y = 69$.

By Art. 89, all the representations belonging to the same set with this are expressed by

$$\begin{aligned} x &= -163t + 991u, \\ y &= \quad 69t - 420u, \end{aligned}$$

where (t, u) is any integral solution of $t^2 - 37u^2 = 1$.

Putting $t = -73 = -T$, $u = -12 = -U$, we obtain the simpler solution $x = 7$, $y = 3$, and hence we derive the general solution in the form

$$\begin{aligned} x &= 7t + 29u, \\ y &= 3t + 24u. \end{aligned}$$

The form $(81, -19, 4)$ is not equivalent to $(3, 1, -12)$, so that the above solution gives all the primitive representations.

The derived representations may be of two kinds, according as $dv(x, y) = 3$ or 9. The former set is deduced from the primitive representations of 9 by $(3, 1, -12)$. Proceeding as before, we obtain the representations of 81 in the form

$$\begin{aligned} x &= -9t + 45u, \\ y &= \quad 3t - 24u, \end{aligned}$$

where, as before, $t^2 - 37u^2 = 1$.

There are no representations for which $dv(x, y) = 9$. This is easily seen from the fact that 1 is representable by the form $(1, 0, -37)$, which is not equivalent to $(3, 1, -12)$.

Improper Equivalence.

92. A few remarks may be added with regard to improper equivalence. Every form is improperly equivalent to its opposite (Art. 62): hence if f is improperly equivalent to f', it is properly equivalent to the opposite of f', and conversely. Moreover, to every proper substitution $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ which converts f into the opposite of f' corresponds an improper substitution $\begin{pmatrix}\alpha, & -\beta\\ \gamma, & -\delta\end{pmatrix}$ which changes f into f', and *vice versa*. Thus the whole theory of improper equivalence is practically reduced to that of proper equivalence.

There is, however, one point of special interest; the forms f and f' may be both properly and improperly equivalent. In this case every form of the class to which f and f' belong is improperly as well as properly equivalent to itself. It may be shown that the necessary and sufficient condition for this is that the class should be ambiguous, that is to say, should contain ambiguous forms.

First, let f, f' be definite: then if we find a reduced form equivalent to them, it must be equivalent to its own opposite, which is also a reduced form. By Art. 65 this is the case only when the reduced form is of the type $(a, \frac{1}{2}a, c)$ or (a, b, a). The first of these is ambiguous; the second is converted by the substitution $\begin{pmatrix}1, & 0\\ 1, & 1\end{pmatrix}$ into the ambiguous form $(2a + 2b, a + b, a)$.

Secondly, suppose that f and f' are indefinite. Let $(a, b, -a')$ be any reduced form in the period of f. By the improper substitution $\begin{pmatrix}0, & 1\\ 1, & 0\end{pmatrix}$ it is converted into its associate $(-a', b, a)$: hence if f, f' are improperly equivalent, their periods must be associated; and if they are properly equivalent as well, their common period must be its own associate, and is therefore ambiguous (Art. 74).

Every ambiguous form is improperly as well as properly equivalent to itself[1]; for if (a, b, c) is ambiguous, and $2b = \beta a$, $\begin{pmatrix} 1, & \beta \\ 0, & -1 \end{pmatrix}$ is an improper automorph. Hence for the double equivalence of two forms it is sufficient as well as necessary that they should belong to an ambiguous class.

93. The effect of an improper automorphic substitution is to interchange the roots of the form to which it is applied (Art. 56); hence if $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$ is an improper automorph of (a, b, c),

$$\frac{-b-\sqrt{D}}{a} = \frac{\alpha(-b+\sqrt{D})+\beta a}{\gamma(-b+\sqrt{D})+\delta a},$$

whence, on multiplying up and equating the rational and irrational parts,

$$a(\alpha+\delta)=0,$$
$$a(b\alpha - a\beta) + b(b\gamma - a\delta) - \gamma D = 0.$$

Now a is not zero; hence

$$\alpha + \delta = 0,$$

and on substituting $-\alpha$ for δ in the second equation we obtain

$$2b\alpha - a\beta + c\gamma = 0.$$

The condition $\alpha\delta - \beta\gamma = -1$ leads to

$$\alpha^2 + \beta\gamma = 1.$$

Since $$a\beta - c\gamma = 2b\alpha,$$

we may put $$a\beta + c\gamma = 2\kappa,$$

where κ is an integer; hence

$$\beta = (\kappa + b\alpha)/a,$$
$$\gamma = (\kappa - b\alpha)/c,$$

and substituting in $\alpha^2 + \beta\gamma = 1$, we obtain

$$\kappa^2 - D\alpha^2 = ac.$$

Thus every improper automorph of (a, b, c) must be of the form

$$\begin{pmatrix} \lambda, & (\kappa+b\lambda)/a \\ (\kappa-b\lambda)/c, & -\lambda \end{pmatrix},$$

where (κ, λ) is an integral solution of $\kappa^2 - D\lambda^2 = ac$. Since

[1] Hence the term 'ambiguous,' which is an unsatisfactory rendering of Gauss's *anceps* = two-headed; cf. 'sacer *ancipiti* mirandus imagine Janus' (Ov. *Fast.* i. 95).

improper automorphs exist for forms belonging to ambiguous classes, and for such forms only, we are led incidentally to the result that if (a, b, c) belongs to an ambiguous class, there will be integral solutions of $\kappa^2 - D\lambda^2 = ac$ for which $(\kappa + b\lambda)/a$ and $(\kappa - b\lambda)/c$ are both integral.

As an illustration, let $(a, b, c) = (2, 5, 7)$. Here $D = 11$, and the values $\kappa = 5$, $\lambda = 1$ lead to the improper automorph $\begin{pmatrix} 1, & 5 \\ 0, & -1 \end{pmatrix}$, from which all the rest may be derived. In like manner the solution $\kappa = 17$, $\lambda = -5$ leads to the improper automorph $\begin{pmatrix} -5, & -4 \\ +6, & +5 \end{pmatrix}$; on the other hand, no improper automorphs can be derived from the solutions $\kappa = 5$, $\lambda = -1$, and $\kappa = 17$, $\lambda = 5$.

CHAPTER IV.

Binary Quadratic Forms; Geometrical Theory.

94. THE theory of the reduction and equivalence of binary quadratic forms is made much more intelligible by the introduction of a complex variable. The discussion of complex quantities belongs to the elements of formal algebra, and will not be reproduced here: for convenience, however, a few of the fundamental results will be stated, and the notation to be used will be explained.

The general form of a complex quantity is

$$z = x + yi,$$

where x, y are real, and $i^2 = -1$.

The *modulus* or *absolute value* of $x + iy$ means $+\sqrt{x^2 + y^2}$. It is denoted by mod $(x + yi)$, or by $|x + yi|$; in what follows, the second notation will be exclusively used.

The square of the modulus of a complex quantity z is called its *norm* and denoted by Nm (z); thus if $z = x + yi$,

$$\text{Nm}\,(z) = x^2 + y^2.$$

The *argument* of $z = x + yi$, denoted by arg (z), is a quantity θ such that $\cos\theta = \frac{x}{|z|}$, $\sin\theta = \frac{y}{|z|}$. It is many-valued, being determined only up to multiples of 2π.

95. If we take an origin O and rectangular axes $X'OX$, $Y'OY$, and mark the point P whose coordinates referred to these axes are x, y, the complex quantity $z = x + yi$ may be considered to be represented either by the point P, or by the vector OP drawn to P from the origin. In particular, 1 and i will be represented by points A, B on OX, OY at unit distance from O. Considered as an operator, $x + yi$ will denote the operation by which the vector $OA = 1$ is converted into the vector $OP = x + yi$.

The modulus and argument of $x + yi$ are equal to the radius vector and vectorial angle of P, if OX be taken as the initial line, and the radian as the unit angle. Calling these r and θ, we have

$$x + yi = r(\cos\theta + i\sin\theta) = re^{\theta i}.$$

96. If $z = x + yi$, and $z' = x' + y'i$, the four fundamental operations are performed according to the formulæ

$$z + z' = (x + x') + (y + y')i = z' + z,$$

$$z - z' = (x - x') + (y - y')i,$$

$$zz' = (xx' - yy') + (xy' + x'y)i = z'z,$$

$$z'/z = \frac{xx' + yy'}{x^2 + y^2} + \frac{(xy' - x'y)}{x^2 + y^2}\, i.$$

Of these, the first and third may be taken as definitions; the second and fourth are derived from them by means of

$$(z - z') + z' = z, \text{ and } \frac{z'}{z} \,.\, z = z'.$$

We shall also require the following results, which are given here for the sake of reference :—

$$|z + z'| \ngtr |z| + |z'|,$$

$$|zz'| = |z|\,|z'|,$$

$$|z/z'| = |z|/|z'|,$$

$$\arg(zz') = \arg(z) + \arg(z'),$$

$$\arg(z/z') = \arg(z) - \arg(z'),$$

$$\log z = \text{Log}\,|z| + i\arg(z).$$

In the last formula, $\text{Log}\,|z|$ means the ordinary real logarithm of the real positive quantity $|z|$.

The quantities $x + yi$ and $x - yi$ are said to be conjugate. It is sometimes convenient to write z_0 for the conjugate of z; it will be observed that $zz_0 = \text{Nm}(z) = \text{Nm}(z_0)$.

97. Consider now the linear transformation of a complex variable defined by

$$z' = \frac{az+b}{cz+d},$$

where a, b, c, d are any constants, in general complex, such that

$$ad - bc \neq 0.$$

This may be regarded as a transformation of the plane of reference by which the point z' is made to correspond to the original point z.

There are, in general, two points which are unaltered by the transformation ; for convenience they may be called the stationary points of the transformation. They correspond to the roots of the equation

$$z = \frac{az+b}{cz+d},$$

or

$$cz^2 + (d-a)z - b = 0.$$

If the roots are z_1 and z_2 the equation of transformation may be written in the 'normal form'

$$\frac{z'-z_1}{z'-z_2} = \lambda \, . \, \frac{z-z_1}{z-z_2}.$$

It is easily seen that $\lambda = (a - cz_1)/(a - cz_2)$, and it may be verified without difficulty that λ satisfies the equation

$$\lambda + \frac{1}{\lambda} = \frac{a^2 + d^2 + 2bc}{ad - bc}.$$

This is a reciprocal quadratic, as might be expected, because the interchange of z_1 and z_2 converts λ into $1/\lambda$. When the roots z_1 and z_2 are distinguished, the value of λ is determined, and conversely.

It may happen that the stationary points coincide : this will be the case when

$$(a-d)^2 + 4bc = 0.$$

Such a substitution is called *parabolic*. It is clear that the values of λ must also coincide, each being equal to 1 ; and, in fact, the equation for λ reduces to

$$\lambda + \frac{1}{\lambda} = 2,$$

whence $(\lambda - 1)^2 = 0$, as stated.

The equation $\dfrac{z'-z_1}{z'-z_2}=\lambda\dfrac{z-z_1}{z-z_2}$ now becomes illusory: it may, however, be replaced by

$$\frac{1}{z'-z_1}=\frac{1}{z-z_1}+k,$$

where $z_1=(a-d)/2c$, $k=2c/(a+d)$.

A special case occurs when $c=0$ and $a-d=0$: here the coincident stationary points are at infinity, and the transformation is

$$z'=z+k,$$

where $k=b/a$.

Observe that k cannot be infinite in either of these last formulæ of transformation: for it will be found that $k=\infty$ leads in each case to $ad-bc=0$, which was expressly excluded at starting.

Those substitutions which are not parabolic may be arranged into three classes, according to the value of λ; namely

(i) *elliptic* substitutions, for which λ is complex, and $|\lambda|=1$,

(ii) *hyperbolic* ,, ,, ,, λ is real, and $\neq 1$,

(iii) *loxodromic* ,, ,, ,, λ is complex, and $|\lambda|\neq 1$.

98. It is a characteristic property of a linear substitution that it transforms circles into circles. This important proposition may be proved as follows.

Since the most general expression for a linear substitution involves three independent quantities, any three assigned values z_1', z_2', z_3' may be made to correspond to any other three z_1, z_2, z_3. In fact, the linear transformation required for this purpose is

$$\frac{z'-z_1'}{z'-z_2'}=\frac{z_3'-z_1'}{z_3'-z_2'}\cdot\frac{z_3-z_2}{z_3-z_1}\cdot\frac{z-z_1}{z-z_2},$$

or, which is the same thing,

$$\frac{z_3'-z_2'}{z_3'-z_1'}\cdot\frac{z'-z_1'}{z'-z_2'}=\frac{z_3-z_2}{z_3-z_1}\cdot\frac{z-z_1}{z-z_2}.$$

It is convenient to write $(\alpha\beta\gamma\delta)$ for $\dfrac{\gamma-\alpha}{\beta-\gamma}\Big/\dfrac{\delta-\alpha}{\beta-\delta}$ and call it a cross-ratio: in this notation, the above substitution may be written

$$(z_1'z_2'z_3'z')=(z_1z_2z_3z).$$

Now if A_1, A_2, A_3, P are the points corresponding to z_1, z_2, z_3, z respectively,

$$|(z_1z_2z_3z)| = \frac{A_1A_3}{A_3A_2} : \frac{A_1P}{PA_2},$$

while
$$\arg(z_1z_2z_3z) = \angle A_1A_3A_2 - \angle A_1PA_2,$$
the angles being described as indicated by the arrows in the figure; that is, by rotating lines from A_3A_1 to A_3A_2, and from PA_1 to PA_2, in the positive sense.

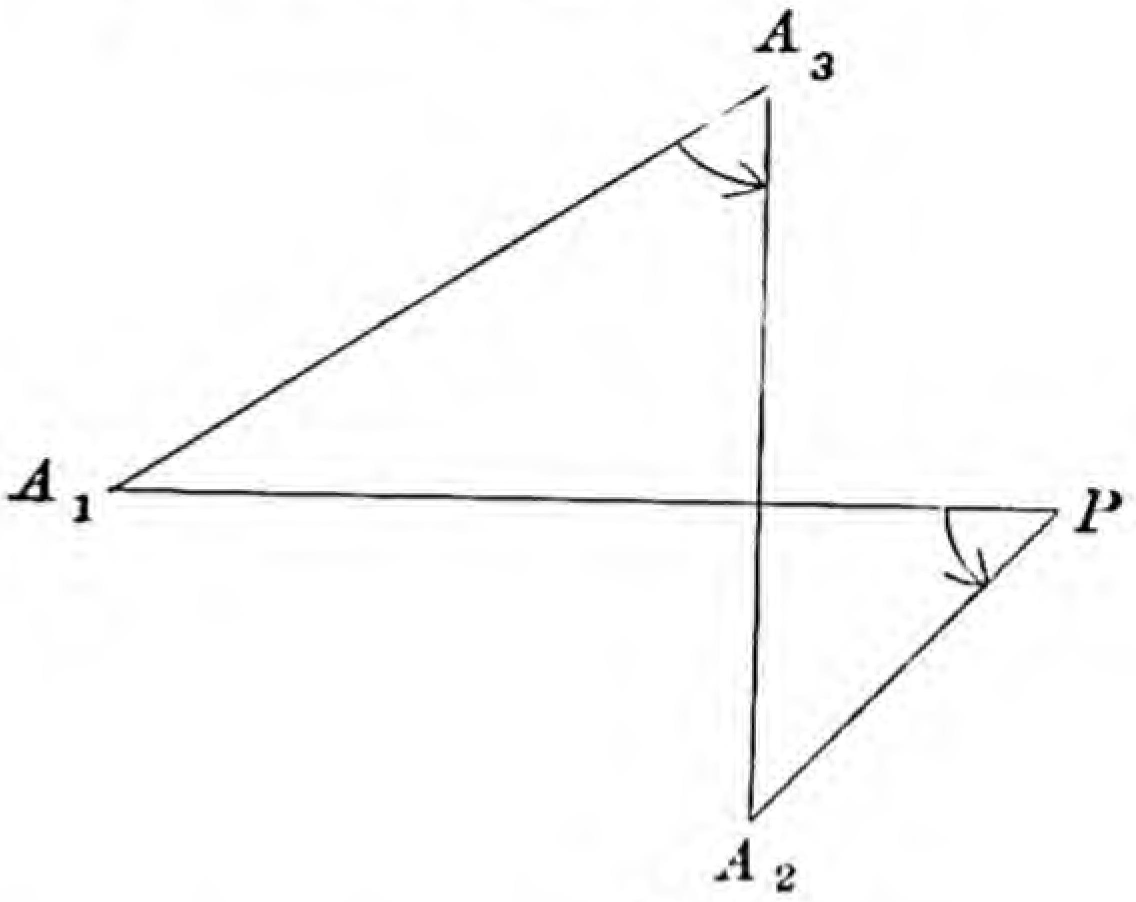

Fig. 2.

It follows from this that $(z_1z_2z_3z)$ is real if and only if

$$P, A_1, A_2, A_3$$

are concyclic; for the condition of reality is that

$$\angle A_1A_3A_2 - \angle A_1PA_2$$

should be a multiple of π, and this is precisely the condition that the four points should be concyclic, the angles being measured as above explained.

When $(z_1z_2z_3z)$ is real, $(z_1'z_2'z_3'z')$ is real also: therefore any point z on the circle $z_1z_2z_3$ is transformed into a point z' on the circle $z_1'z_2'z_3'$.

It should be observed that, in this connexion, straight lines are to be considered as equivalent to circles of infinite radius; in fact a straight line is in general transformed into a circle, and a circle may be (exceptionally) transformed into a straight line.

99. In the arithmetical application, it will be sufficient, for the present, to consider the substitutions

$$z' = \frac{\alpha z + \beta}{\gamma z + \delta},$$

where $\alpha, \beta, \gamma, \delta$ are real integers such that $\alpha\delta - \beta\gamma = 1$.

The equation for λ is in this case (Art. 97)

$$\lambda + \lambda^{-1} = \alpha^2 + \delta^2 + 2\beta\gamma$$
$$= (\alpha + \delta)^2 - 2.$$

The discriminant of this quadratic is

$$4 - \{(\alpha+\delta)^2 - 2\}^2 = (\alpha+\delta)^2\{4 - (\alpha+\delta)^2\}.$$

This is negative, and the substitution is hyperbolic, except in the following cases:—

I. $\alpha + \delta = 0$, whence also $\beta\gamma + \alpha^2 + 1 = 0$.

Here the equation for λ is $(\lambda + 1)^2 = 0$, and the stationary points are the roots of

$$\gamma z^2 - 2\alpha z - \beta = 0,$$

whence

$$z = (\alpha \pm i)/\gamma.$$

The substitution may be written in the form

$$\frac{z' - (\alpha + i)/\gamma}{z' - (\alpha - i)/\gamma} = -\frac{z - (\alpha + i)/\gamma}{z - (\alpha - i)/\gamma},$$

from which we see that it is elliptic and of period 2.

II. $(\alpha + \delta)^2 = 1$.

It is enough to suppose that $\alpha + \delta = 1$, because if $\alpha + \delta = -1$, we can change the signs of $\alpha, \beta, \gamma, \delta$ throughout, without altering the substitution.

The equation for λ is

$$\lambda^2 + \lambda + 1 = 0,$$

and therefore, putting $\rho = e^{2\pi i/3} = \dfrac{-1 + i\sqrt{3}}{2}$,

$$\lambda = \rho \text{ or } \rho^2.$$

The equation for the stationary points is

$$\gamma z^2 - (2\alpha - 1) z - \beta = 0,$$

whence

$$z = \frac{2\alpha - 1 \pm \sqrt{(2\alpha - 1)^2 + 4(\alpha\delta - 1)}}{2\gamma}$$
$$= \frac{2\alpha - 1 \pm i\sqrt{3}}{2\gamma} \text{ on reduction}$$
$$= \frac{\alpha + \rho}{\gamma} \text{ or } \frac{\alpha + \rho^2}{\gamma}.$$

If we take $\lambda = \rho$, we must put (Art. 97)

$$z_1 = \frac{\alpha + \rho^2}{\gamma}, \qquad z_2 = \frac{\alpha + \rho}{\gamma},$$

and the normal form of the substitution is

$$\frac{z' - (\alpha + \rho^2)/\gamma}{z' - (\alpha + \rho)/\gamma} = \rho \cdot \frac{z - (\alpha + \rho^2)/\gamma}{z - (\alpha + \rho)/\gamma}.$$

This is elliptic, and of period 3. The other substitution of the same period is obtained from the preceding by changing ρ into ρ^2.

III. $\alpha + \delta = 2$.

Here $(\lambda - 1)^2 = 0$, and the equation for the stationary points is

$$\gamma z^2 - 2(\alpha - 1) z + \frac{(\alpha - 1)^2}{\gamma} = 0,$$

or

$$\gamma \left(z - \frac{\alpha - 1}{\gamma} \right)^2 = 0.$$

The substitution is parabolic, and may be written

$$\frac{1}{z' - (\alpha - 1)/\gamma} = \frac{1}{z - (\alpha - 1)/\gamma} + \gamma.$$

If it happens that $\gamma = 0$, we must have $\alpha = \delta = 1$, and the substitution becomes

$$z' = z + \beta.$$

All the remaining substitutions are hyperbolic, the stationary points being defined by

$$\gamma z^2 - (\alpha - \delta) z - \beta = 0.$$

100. As in last chapter, it may be shown that to every quadratic equation with integral coefficients and real roots corresponds a group of hyperbolic substitutions which have the roots of the equation for their stationary points. Namely, if the equation is reduced to the form $az^2 + 2bz + c = 0$, where

$$dv(a, b, c) = 1,$$

and if we put as usual $b^2 - ac = D$, $dv(a, 2b, c) = \sigma$, the substitutions in question will be given by

$$\frac{z' - z_1}{z' - z_2} = \left(\frac{t + u\sqrt{D}}{\sigma} \right)^2 \cdot \frac{z - z_1}{z - z_2},$$

where (t, u) is any integral solution of $t^2 - Du^2 = \sigma^2$, and z_1, z_2 are the roots of $az^2 + 2bz + c = 0$.

(It is left as an exercise to the reader to verify that the normal form of the substitution here given is only a transformation of $z' = \frac{(t-bu)z - cu}{auz + (t+bu)}$. It is interesting to see that the squared factor ensures that λ and λ^{-1} are both positive, as they ought to be, because $\lambda + \lambda^{-1} = (\alpha + \delta)^2 - 2$, which is positive.)

101. Points which can be stationary points for a substitution of the complete group may be called *critical* points; it appears that they fall into four sets, which may be termed respectively

(i) rational points, for which $z = p/q$,

(ii) surd points " " $z = (p \pm \sqrt{q})/r$,

(iii) i-points " " $z = (p \pm i)/q$,

(iv) ρ-points " " $z = (p \pm \rho)/q$.

Here p, q, r denote real integers; in (iii), p and q must be relative primes; in (iv), with the upper sign p and q must be relative primes, and with the lower sign $p+1$ and q must be relative primes.

102. A complex quantity $z = x + yi$ for which $y > 0$ will be said to have a positive imaginary part; its representative point will be on the positive side of the axis of x.

Two quantities z, z' will be termed *equivalent* when real integers α, β, γ, δ can be found such that

$$z' = \frac{\alpha z + \beta}{\gamma z + \delta},$$

$$\alpha\delta - \beta\gamma = 1.$$

The corresponding points will also be called equivalent.

Equivalent points are on the same side of the axis of x.

For suppose that $z' = \frac{\alpha z + \beta}{\gamma z + \delta}$ as above, and let z_0, z_0' be the conjugates of z and z': then

$$z_0' = \frac{\alpha z_0 + \beta}{\gamma z_0 + \delta},$$

and therefore

$$z' - z_0' = \frac{(\alpha\delta - \beta\gamma)(z - z_0)}{(\gamma z + \delta)(\gamma z_0 + \delta)}$$

$$= \frac{z - z_0}{\mathrm{Nm}(\gamma z + \delta)}.$$

If $z=x+yi$ and $z'=x'+y'i$, this gives $y/y'=\mathrm{Nm}\,(\gamma z+\delta)$, a positive quantity, so that y and y' have the same sign.

If $y=0$, $y'=0$ also; that is, a quantity equivalent to a real quantity is also real.

103. Suppose now that $\omega=x+yi$ is any complex quantity with positive imaginary part, and let $\omega_0=x-yi$ be its conjugate.

Consider the points ω which satisfy the conditions

$$|\,\omega+\omega_0\,|<1,$$

$$\omega\omega_0>1.$$

Expressed in terms of x and y these are

$$2\,|\,x\,|<1,$$

$$x^2+y^2>1.$$

Now the points (x, y) for which $2\,|\,x\,|<1$, $x^2+y^2>1$, $y>0$ are all contained within the area which lies above the axis of x, outside the unit circle $x^2+y^2-1=0$ and between the parallel lines $x=\frac{1}{2}$ and $x=-\frac{1}{2}$. (See the annexed figure, in which the area in question is shaded.)

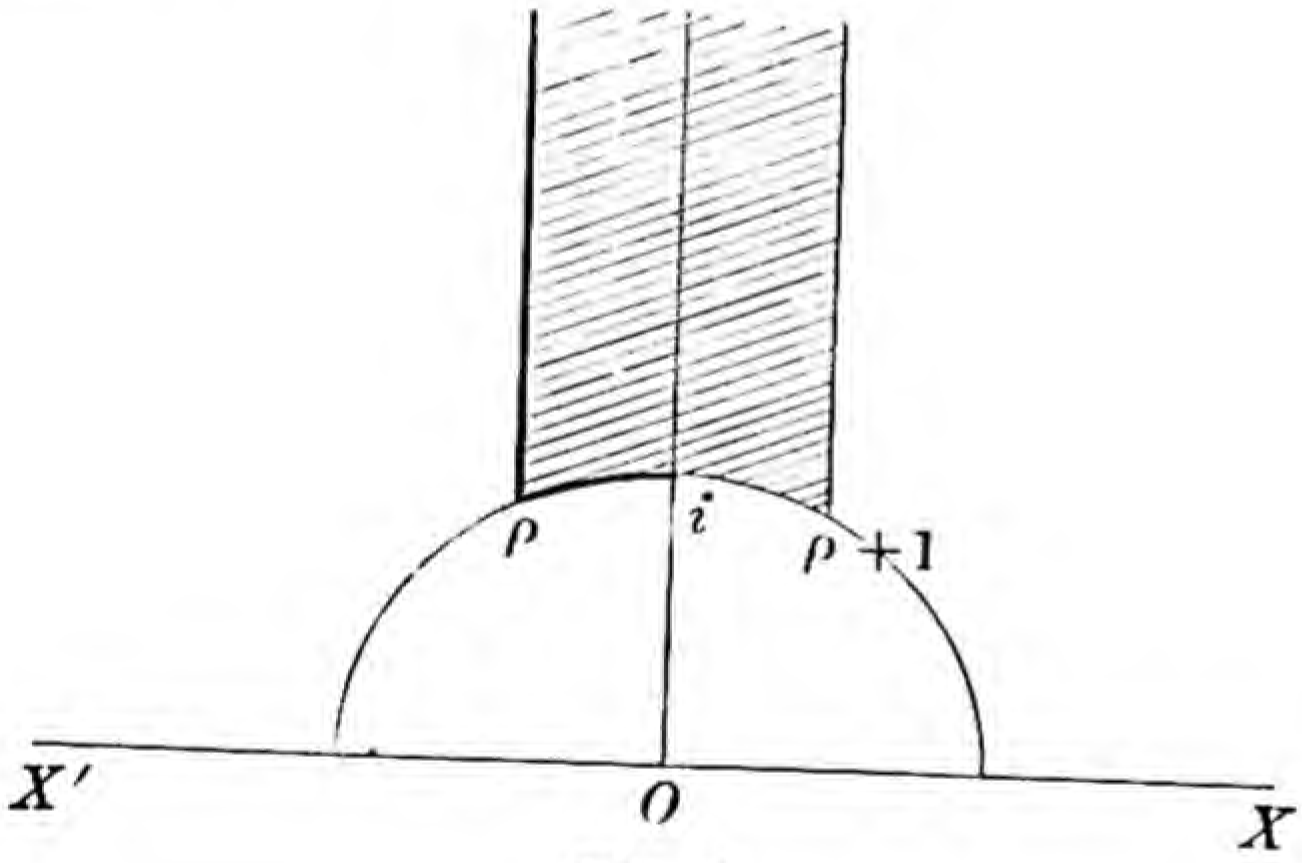

Fig. 3.

This region may be considered as a triangle enclosed by three circular arcs (two of which are accidentally straight), the angles of the triangle being 0, $\pi/3$, $\pi/3$. It will be referred to as the *fundamental triangle*, and denoted by ∇.

104. *The points on the boundary of* ∇ *may be grouped into equivalent pairs.*

For it is evident that the transformation

$$\omega'=S(\omega)=\omega+1$$

converts every point ω on the line $x = -\frac{1}{2}$ into a corresponding point ω' on $x = \frac{1}{2}$, and if one of these is on the boundary of ∇, so is the other. Also the transformation

$$\omega' = T(\omega) = -1/\omega,$$

or, which is the same thing,

$$x' + y'i = \frac{-x + yi}{x^2 + y^2}$$

converts every point ω on the circular arc extending from ρ to i into a point ω' on the arc from i to $(1 + \rho)$.

A point will be called a *reduced* point if it is either within ∇ or on that half of the boundary of ∇ which is on the negative side of the axis of y. The point i is included.

The reduced points ρ, i are critical. The third vertex of ∇, which is at infinity, may also be considered a critical point for the substitution $S(\omega) = \omega + 1$.

This seems the proper place to observe that *from our present point of view* $z = \infty$ simply means that the absolute value of z is infinite, and we shall have no reason to distinguish between (say) $z = \infty$, a real quantity, and $z = \infty\, i$, a pure imaginary. We shall therefore speak of *the point* ∞. Perhaps the reader may be assisted by considering the effect of inverting the plane of reference into a sphere: to every accessible point on the plane will correspond one point on the sphere, but all the infinite elements of the plane will be represented by a single point on the sphere, and this representation will be sufficient *so long as* $z = \infty$ *can be used without distinction for any quantity of which the norm is infinitely great.* This is the case, for instance, in the theory of algebraic integrals and Abelian functions as expounded by Riemann. On the other hand, if we distinguish those complex quantities $z = x + yi$ for which $\mathrm{Nm}(z)$ is infinite, according to the ratio of x to y, our 'infinite' elements will form a linear multiplicity. This is what is done in plane projective geometry, and it is for this reason that we speak of 'the straight line at infinity in a plane.' A great deal of misunderstanding is avoided if it be remembered that the terms *infinity, infinite, zero, infinitesimal* must be interpreted in connexion with their context, and admit of a variety of meanings according to the way in which they are defined.

105. *There are no reduced critical points except* i, ρ, ∞, *the vertices of the fundamental triangle.*

For if we put $\omega = (\alpha + i)/\gamma$, the conditions that ω should belong to the fundamental triangle are

$$\gamma > 0, \quad \left|\frac{\alpha}{\gamma}\right| \not> \tfrac{1}{2}, \quad \alpha^2 + 1 \not< \gamma^2,$$

and the only integral solution is $\alpha = 0$, $\gamma = 1$, whence $\omega = i$.

Similarly $\omega = (\alpha + \rho)/\gamma$ is reduced only if $\alpha = 0$, $\gamma = 1$ or $\alpha = 1$, $\gamma = 1$; and of the two points ρ, $1 + \rho$ only ρ is reduced.

Obviously no rational or surd points can be reduced.

106. *No two reduced points can be equivalent.*

Suppose, if possible, that

$$\omega \text{ and } \omega' = \frac{\alpha\omega + \beta}{\gamma\omega + \delta}$$

are both reduced.

We have (by Art. 102)

$$\omega' - \omega_0' = \frac{\omega - \omega_0}{\text{Nm}(\gamma\omega + \delta)};$$

now

$$\begin{aligned} \text{Nm}(\gamma\omega + \delta) &= \gamma^2\omega\omega_0 + \gamma\delta(\omega + \omega_0) + \delta^2 \\ &> \gamma^2 - \gamma\delta + \delta^2 \\ &> 1, \end{aligned}$$

with a possible exception when either $\gamma = 0$, $\delta = \pm 1$, or $\gamma = \pm 1$, $\delta = 0$. Hence, with these possible exceptions,

$$|\omega' - \omega_0'| < |\omega - \omega_0|.$$

But since

$$\omega = \frac{\delta\omega' - \beta}{-\gamma\omega' + \alpha}$$

and ω' is reduced, we have in the same way

$$|\omega - \omega_0| < |\omega' - \omega_0'|,$$

except perhaps when either $\gamma = 0$, $\alpha = \pm 1$, or $\alpha = 0$, $\gamma = \pm 1$.

It is impossible that $|\omega' - \omega_0'| < |\omega - \omega_0|$ and

$$|\omega' - \omega_0'| > |\omega - \omega_0|$$

simultaneously. Hence it is sufficient to examine the cases

$$\gamma = 0, \qquad \alpha = \delta = 1$$

and

$$\gamma = \pm 1, \qquad \alpha = \delta = 0,$$

whence also

$$\beta = \mp 1.$$

The first case gives $\omega' = \omega + \beta$,

so that if (x, y) are the coordinates of the point ω, those of ω' will be $(x + \beta, y)$. Now β is at least equal to 1 numerically, and since the width of ∇ is just equal to 1, it follows that ω and ω' cannot both be reduced.

In the second case $\omega' = -1/\omega$,

whence

$$\text{Nm}(\omega) \,.\, \text{Nm}(\omega') = 1.$$

If $\text{Nm}(\omega) > 1$, $\text{Nm}(\omega') < 1$ and ω' cannot be reduced: similarly if $\text{Nm}(\omega') > 1$, ω is not reduced. If $\text{Nm}(\omega) = 1$, ω can only be on the circular arc going from ρ to i, and then $\omega' = -1/\omega$ is on the arc going from i to $\rho + 1$, and is consequently not reduced. (Cf. Art. 104.)

107. We shall now state and prove a proposition the object of which may not be very evident: it is, in fact, preparatory to the important theorem which follows it.

Within the area, above the axis of x, which is enclosed by the parallel lines $x = \pm\frac{1}{2}$ and the line $y = c$, where c is a finite positive quantity, there can only be a finite number of points equivalent to a given point ω, the ordinate of which exceeds c.

Let $\omega = \xi + \eta i$, where $\eta > c$.

Then if $\omega' = \dfrac{\alpha\omega + \beta}{\gamma\omega + \delta} = x + yi$ be an equivalent point,

$$y = \frac{1}{2i}(\omega' - \omega_0') = \frac{\eta}{\gamma^2(\xi^2 + \eta^2) + 2\gamma\delta\xi + \delta^2}.$$

Therefore if $y > c$,

$$\gamma^2(\xi^2 + \eta^2) + 2\gamma\delta\xi + \delta^2 < \eta/c,$$

that is,

$$(\xi\gamma + \delta)^2 + \eta^2\gamma^2 < \eta/c.$$

Now since the expression on the left-hand side is the sum of two squares and ξ, η are real, it is clear that only a limited number of real integers γ, δ can be found to satisfy the inequality.

Suppose that (γ', δ') is any suitable pair of values, γ', δ' being relative primes. Then if α', β' are any integers such that

$$\alpha'\delta' - \beta'\gamma' = 1,$$

the most general solution of $\alpha\delta' - \beta\gamma' = 1$ is

$$\alpha = \alpha' + m\gamma',$$

$$\beta = \beta' + m\delta',$$

m being any integer.

Hence

$$\omega' = \frac{\alpha\omega + \beta}{\gamma'\omega + \delta'} = \frac{\alpha'\omega + \beta'}{\gamma'\omega + \delta'} + m.$$

Suppose, now, that we consider points on the boundary $x = -\frac{1}{2}$ as belonging to the area defined in the enunciation, but points on $x = +\frac{1}{2}$ as being outside of it. Then it is possible in one way only to determine the integer m so that the conditions

$$-\tfrac{1}{2} \leqq x' < \tfrac{1}{2}$$

may be satisfied. Therefore for every combination (γ', δ') in which γ', δ' are relative primes, and $(\gamma'\xi + \delta')^2 + \gamma'^2\eta^2 < \eta/c$, we obtain one and only one point ω', equivalent to ω, within the area defined by $-\frac{1}{2} \overline{\overline{<}} x' < \frac{1}{2}$, $y' > c$. The number of these points is therefore finite.

108. We are now able to prove the fundamental proposition, that

Every point above the axis of x is equivalent to one and only one reduced point.

Let $\omega = \xi + \eta i$, where $\eta > 0$.

The integer m may be uniquely determined so that

$$-\tfrac{1}{2} \overline{\overline{<}} \xi + m < \tfrac{1}{2}.$$

Put

$$\omega' = \omega + m :$$

then if $|\omega'| > 1$, ω' is reduced: if not, let

$$\omega'' = -1/\omega ;$$

then the ordinate of $\omega'' = \eta/\mathrm{Nm}\,(\omega') > \eta$, except when $\mathrm{Nm}\,(\omega') = 1$. If $\mathrm{Nm}\,(\omega') = 1$, either ω' or ω'' is reduced. If otherwise, let m' be chosen so that

$$\omega''' = \omega'' + m' = x''' + y'''i$$

satisfies the conditions

$$-\tfrac{1}{2} \overline{\overline{<}} x''' < \tfrac{1}{2} ;$$

and if ω''' is not yet reduced put $\omega^{\text{iv}} = -1/\omega'''$. Then, as before, the ordinate of ω^{iv} exceeds that of ω''' and *a fortiori* that of ω. By proceeding in this way we must at last arrive at a reduced point, because the points ω', ω''', etc., all lie within the area defined by

$$-\tfrac{1}{2} \overline{\overline{<}} x < \tfrac{1}{2}, \quad y > \eta,$$

and by the preceding lemma this area contains only a finite number of points equivalent to ω.

Thus it has been proved that to every point ω above the axis of x an equivalent reduced point can be found. Further, if ω were equivalent to two different reduced points, these reduced points would be equivalent to each other; but this has been proved to be impossible (Art. 106); therefore the reduction is unique.

109. *If a non-critical reduced point is transformed by two different substitutions* $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$, $\begin{pmatrix}\alpha', & \beta'\\ \gamma', & \delta'\end{pmatrix}$ *the transformed points cannot be identical.*

For if they were, the substitution

$$\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}\begin{pmatrix}\delta', & -\beta'\\ -\gamma', & \alpha'\end{pmatrix},$$

which is not identical, would transform the reduced point into itself; but this is impossible.

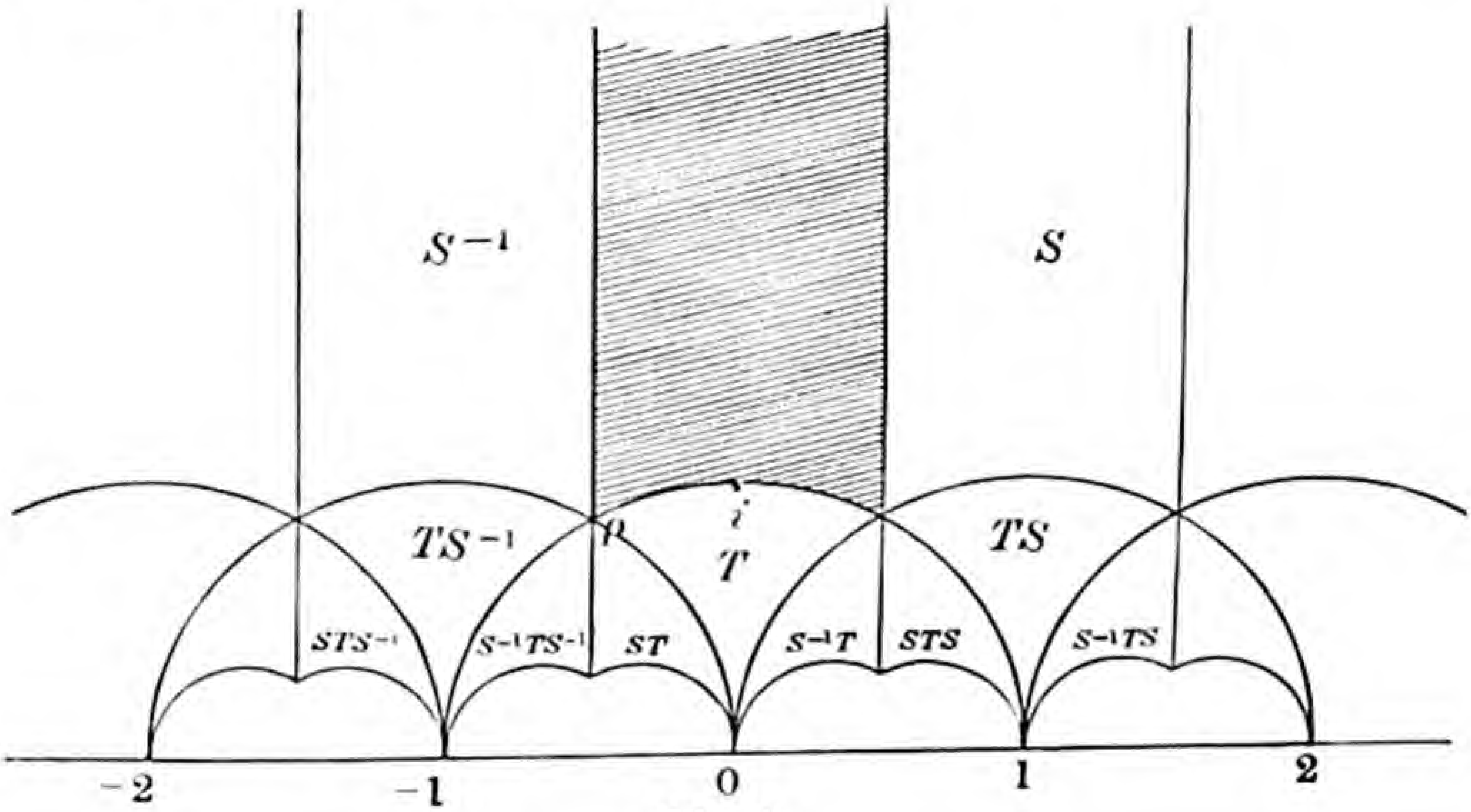

Fig. 4.

110. It follows from the propositions just proved that by means of the group of proper unitary substitutions, that part of the plane of reference which lies above the axis of real quantities is divided up into an infinite number of equivalent triangles. A few of these are shown in the figure, where, as before, the fundamental triangle is shaded. The triangles fill up the half-plane completely, without overlapping: as we approach the axis of abscissæ, the triangles become smaller and smaller, and are ultimately infinitesimal. Every rational point on the axis of x is the common vertex of an infinity of triangles; no other point on this axis belongs to any of the triangles.

It may be observed that the whole number of triangles is an infinity comparable with n^3, where n is an indefinitely large positive integer.

The propositions which immediately follow are intuitively evident from the figure; they may be rigorously proved with the aid of the preceding articles.

Every triangle is surrounded by three adjacent triangles, each of which is separated from it by one of its sides.

Every ρ-point is a common vertex of six contiguous triangles.

The angles of every triangle are $0, \pi/3, \pi/3$, and its vertices are at a rational point and two ρ-points respectively.

111. Suppose that a sphere is drawn touching the plane of reference at the origin O; and let the figure be projected stereographically upon the sphere from the point diametrically opposite to O. Then the triangles in the plane are projected into triangles on the sphere bounded by arcs of small circles; and we have the whole surface of a hemisphere divided up into a series of triangles, which may be considered equivalent as before (cf. Art. 104). In particular, the size of the sphere may be so arranged that the point i in the plane is projected into the pole of the great circle which bounds the hemisphere; the spherical figure then becomes symmetrical.

112. The whole theory of the reduction of definite quadratic forms may now be summed up by saying that a reduced form is one of which the principal root corresponds to a point which belongs to the fundamental triangle; and that Lagrange's process of reduction is a methodical way of discovering the substitution whereby the triangle in which the principal root of any given form may lie is transformed into the fundamental triangle.

The successive substitutions by which the reduction is effected are all of the type

$$\omega = \delta - 1/\omega', \quad \text{or} \quad \omega' = 1/(\delta - \omega);$$

and this may be considered as compounded of

$$\omega_1 = \omega - \delta$$

and

$$\omega' = -1/\omega_1.$$

Now the substitution $\omega_1 = \omega - \delta$ is the $(-\delta)$th power of $\omega' = \omega + 1$; so that we have incidentally a proof of the important proposition that

Every proper unitary substitution may be expressed as a product of powers of the elementary substitutions

$$S = \begin{pmatrix} 1, & 1 \\ 0, & 1 \end{pmatrix}, \qquad (\omega' = \omega + 1),$$

$$T = \begin{pmatrix} 0, & -1 \\ 1, & 0 \end{pmatrix}, \qquad (\omega' = -1/\omega).$$

The substitution S, which is parabolic, corresponds to a translation through unit distance parallel to the axis of x. The substitution T, which is elliptic, and of period 2, is equivalent to inversion with respect to the unit-circle

$$x^2+y^2-1=0$$

followed by reflexion with respect to the axis of y.

The substitution $ST=\begin{pmatrix}1, & -1\\ 1, & 0\end{pmatrix}$ or $\omega'=(\omega-1)/\omega$ is elliptic and of period 3: for it may be written

$$\frac{\omega'-(\rho+1)}{\omega'+\rho}=\rho^2\frac{\omega-(\rho+1)}{\omega+\rho}.$$

Hence $(ST)^3=1$; that is, $STSTST=1$. Besides this, and $T^2=1$, there are no other independent identical relations connecting S and T; this follows from the fact that the critical points with elliptic substitutions may be arranged in the two groups of i-points and ρ-points (cf. Art. 99). Each identical relation may be deduced by making a circuit round an i-point or a ρ-point, as the case may be.

113. Within each triangle in fig. 4 is written a symbol for the geometrical transformation by which it is derived from ∇. It should be observed that on account of $STSTST=1$, and $T^2=1$, the transformations may be written in a great variety of ways; also that the order of composition of the geometrical operations S, T is from left to right; thus, when TS is placed inside a triangle it means that this is derived from ∇ by *first* performing the operation T, and then the operation S.

It should also be observed that, in conformity with the definitions of Art. 57, the substitution $\omega'=ST(\omega)$ means the result of combining

$$\omega'=\omega_1+1$$

and

$$\omega_1=-1/\omega,$$

so that the substitution $\omega'=ST(\omega)$ connects with a reduced point ω a point ω' within the triangle marked TS in the figure (not ST): and, in general, to obtain the algebraical substitution $\omega'=R(\omega)$, which converts a reduced point ω into any point ω', we must reverse the symbol written in the triangle to which ω' belongs.

114. We will now proceed to discuss the reduction of indefinite forms.

The roots ω_1, ω_2 of a primitive indefinite form (a, b, c) of determinant D are surd critical points, being unaltered by the group of hyperbolic substitutions

$$\begin{pmatrix}(t-bu)/\sigma, & -cu/\sigma \\ au/\sigma, & (t+bu)/\sigma\end{pmatrix},$$

where $t^2 - Du^2 = \sigma^2$, and $dv\,(a, 2b, c) = \sigma$ (Arts. 82, 83).

Now let a circle be described on the segment $\omega_1\omega_2$ as diameter. Its equation is

$$a\,(x^2+y^2) + 2bx + c = 0.$$

This circle will intersect an infinite number of equivalent triangles in the half-plane above $y = 0$. If one of these is the fundamental triangle, the form (a, b, c) is said to be reduced.

The condition for a reduced form is evidently that one at least of the points ρ, $1+\rho$ should fall within the circle

$$a\,(x^2+y^2) + 2bx + c = 0.$$

This leads to
$$a\,(a \pm b + c) < 0,$$
or, on substituting $(b^2 - D)/a$ for c, and observing that D is positive,

$$a^2 \pm ab + b^2 < D.$$

This may be written

$$(2a \pm b)^2 + 3b^2 < 4D,$$

from which it is clear that only a limited number of integers a, b can be found to satisfy the inequality. *Therefore the number of reduced forms is finite.*

115. If we operate on a reduced form (a, b, c) with the substitution $S = \begin{pmatrix}1, & 1 \\ 0, & 1\end{pmatrix}$, we obtain (a, b', c'), where

$$b' = b + a,$$
$$c' = a + 2b + c;$$

hence
$$a\,(a - b' + c') = a\,(a + b + c),$$
so that if $a\,(a+b+c) < 0$, $a\,(a - b' + c') < 0$, and (a, b', c') is reduced.

Similarly, the operation $S^{-1} = \begin{pmatrix} 1, & -1 \\ 0, & 1 \end{pmatrix}$ leads to (a, b', c') with

$$b' = b - a,$$
$$c' = a - 2b + c,$$

whence $a(a + b' + c') = a(a - b + c)$: therefore if $a(a - b + c) < 0$, (a, b', c') is reduced.

Suppose now that $a(a + b + c) > 0$, and $a(a - b + c) < 0$; then the form $(c, -b, a)$, derived from (a, b, c) by the substitution $T = \begin{pmatrix} 0, & -1 \\ 1, & 0 \end{pmatrix}$, will be reduced. For it is clear that $(a + b + c)$ and $(a - b + c)$ have opposite signs: hence either $c(c + b + a)$ or $c(c - b + a)$ is negative.

The same conclusion follows if

$$a(a + b + c) < 0 \text{ and } a(a - b + c) > 0.$$

Therefore if (a, b, c) is any reduced form there will be, in general, two adjacent reduced forms equivalent to it; if $(a + b + c)$ and $(a - b + c)$ have the same sign, these forms are derived from (a, b, c) by the substitutions S and S^{-1}; while if $(a + b + c)$ and $(a - b + c)$ differ in sign, the substitutions are T and either S or S^{-1} according as $a(a + b + c)$ or $a(a - b + c)$ is negative.

116. It may happen that one of the quantities $a(a \pm b + c)$ is negative, while the other vanishes; in this case (a, b, c) will be called a *critical* form. Its representative circle passes through one of the points ρ, $\rho + 1$ and includes the other. We have $a^2 \pm ab + b^2 = D$, so that these critical forms will only occur when $2D$ can be represented by the form $(2, 1, 2)$.

Suppose that (a, b, c) is a critical form with $a + b + c = 0$ and $a(a - b + c) < 0$: then ab is positive. The substitution S changes (a, b, c) into $(a, -c, b)$ which is not reduced, because

$$a(a - c + b) = 2a(a + b),$$

which is positive. Similarly the substitution T converts (a, b, c) into $(c, -b, a)$, which is not reduced, because

$$c(c - b + a) = 2b(a + b) = +.$$

On the other hand S^{-1} converts (a, b, c) into $(a, b - a, -3b)$ which is reduced, because $a(a + b - a - 3b) = -2ab = -$, and is not critical except when $a = 2b$.

Moreover, the substitution $STS = \begin{pmatrix} 1, & 0 \\ 1, & 1 \end{pmatrix}$ converts (a, b, c) into $(b, -a, c)$, which is also critical, and then S transforms this into $(b, b-a, -3a)$, which is reduced but not critical, except when $b = 2a$.

Now if $a = 2b$, $c = -3b$, and the form is $(2b, b, -3b)$: this is primitive only when $b = \pm 1$: and similarly the primitive critical forms for which $b = 2a$, $a + b + c = 0$ are $(\pm 1, \pm 2, \mp 3)$. Therefore with the single exception of $D = 7$, we are able to associate each critical form with two other reduced forms, one of which is critical, and the other not.

Exactly similar reasoning applies to the other case of critical forms. The final conclusion is that the reduced forms may be arranged in periods such that each form is converted into the next following by one or other of the five substitutions

$$S,\ S^{-1},\ T,\ STS,\ S^{-1}TS^{-1},$$

where the last two are only to be applied to critical forms.

Observe that $S^{-1}TS^{-1} = \begin{pmatrix} 1, & 0 \\ -1, & 1 \end{pmatrix} = (STS)^{-1} = TST$; hence if we put U for STS, the five substitutions are S, S^{-1}, T, U, U^{-1}.

An example will make this clearer. If $D = 37$, the periods of reduced forms for the classes represented by $(1, 0, -37)$, $(3, 1, -12)$ are

I. $(1, 0, -37)$, $(1, 1, -36)$, $(1, 2, -33)$, $(1, 3, -28)$,
$(1, 4, -21)$, $(1, 5, -12)$, $(1, 6, -1)$, $(-1, -6, 1)$,
$(-1, -5, 12)$,...$(-1, 6, 1)$, $(1, -6, -1)$, $(1, -5, 12)$,...
$(1, -1, 36)$.

II. $(3, 1, -12)$, $(3, 4, -7)$*, $(4, -3, -7)$*, $(4, 1, -9)$,
$(4, 5, -3)$, $(-3, -5, 4)$, $(-3, -2, 11)$, $(-3, 1, 12)$,
$(-3, 4, 7)$*, $(-4, -3, 7)$*, $(-4, 1, 9)$, $(-4, 5, 3)$,
$(3, -5, -4)$, $(3, -2, 11)$.

In the second period the critical form $(3, 4, -7)$ is converted into $(4, -3, -7)$ by STS, and $(-3, 4, 7)$ into $(-4, -3, 7)$ by $S^{-1}TS^{-1}$.

117. In tabulating periods of reduced forms, we may omit those forms which are connected with both the adjacent ones by the substitutions S, S^{-1}; the remaining forms may be called principal reduced forms. Thus, for the two periods given above, the principal reduced forms are

I. $(1, 6, -1)$, $(-1, -6, 1)$, $(-1, 6, 1)$, $(1, -6, -1)$.

II. $(3, 4, -7)$, $(4, -3, -7)$, $(4, 5, -3)$, $(-3, -5, 4)$,
$(-3, 4, 7)$, $(-4, -3, 7)$, $(-4, 5, 3)$, $(3, -5, -4)$.

The characteristics of a principal reduced form (a, b, c) are that either $a+b+c$ and $a-b+c$ have opposite signs, or if one of them vanishes, the other has a sign opposite to a. Geometrically, the representative circle of a principal reduced form includes one of the points ρ, $\rho+1$, and either excludes or passes through the other.

For the exceptional case $D=7$, there are two periods of principal reduced forms: of these one is

$(1, -2, -3)$, $(1, 2, -3)$, $(2, -1, -3)$,
$(2, 1, -3)$,

and the other is obtained by changing the signs of the coefficients throughout. All the principal reduced forms are critical.

118. Every form is equivalent to at least one reduced form. For suppose the representative circle of the form constructed: this will intersect an infinite number of triangles, and the substitution which transforms any one of these into the fundamental triangle will convert the given form into an equivalent reduced form.

119. It may be proved by considerations similar to those adduced in Chap. III. that two equivalent reduced forms must belong to the same period. It does not seem worth while to give the proof in detail: it may be observed, however, that with regard to the automorphs derived from the periods, and the corresponding chain-fractions obtained from them, a distinction has to be made between periods which contain critical forms and those which do not.

Thus for $D=37$ the non-critical period

$(1, 6, -1)$, $(-1, -6, 1)$, $(-1, 6, 1)$, $(1, -6, -1)$

leads to an automorph of $(1, 6, -1)$ in the form

$$TS^{-12}TS^{12} = \begin{pmatrix} 1, & 12 \\ 12, & 145 \end{pmatrix},$$

and exactly as in the Gaussian theory we obtain from this the expansion

$$\sqrt{37} - 6 = (0;\ \overset{*}{12}).$$

On the other hand, the period of $(3, 4, -7)$ leads to the automorph $STS^3TS^{-4}TS^{-3}TS^3 = \begin{pmatrix} 25, & 84 \\ 36, & 121 \end{pmatrix}$, and the corresponding expansion

$$\frac{\sqrt{37} - 4}{3} = (1;\ -\overset{*}{3},\ -4,\ 3,\ \overset{*}{4}).$$

120. In conclusion, a word may be said about the geometrical meaning of the automorphic substitutions. The infinity of triangles which have a common vertex at a rational point may be said to form a *sheaf* of triangles. In particular, those which have a common vertex at infinity may be said to constitute the *primary* sheaf.

Suppose now that Σ' is a sheaf with its vertex at the rational point $-\delta/\gamma$, where γ, δ may be taken as relative primes. Determine α, β so that $\alpha\delta - \beta\gamma = 1$; then the substitution

$$\omega' = \frac{\alpha\omega + \beta}{\gamma\omega + \delta}$$

will transfer the point $-\delta/\gamma$ to infinity, and Σ' will therefore be transformed into the primary sheaf Σ.

The most general substitution by which this is effected is

$$\begin{aligned} \omega'' &= \frac{(\alpha + m\gamma)\,\omega + (\beta + m\delta)}{\gamma\omega + \delta} \\ &= \omega' + m, \end{aligned}$$

where m is any integer.

Now the substitution $\omega'' = \omega' + m$ simply produces a cyclical permutation of the triangles of the primary sheaf: hence we see that it is always possible, and in one way only, to transform any sheaf Σ' into the primary sheaf so that any assigned triangle of Σ' may become the fundamental triangle ∇. More generally, any sheaf Σ' may be uniquely transformed into any other, Σ'', so that any assigned triangle of Σ' may be converted into an assigned triangle of Σ''.

It is now evident that the representative circle of any form will intersect the same number of triangles in every sheaf which it crosses: this number being equal to the number of reduced forms in its complete period as defined in Art. 116.

The effect of applying an automorphic substitution is to produce a cyclical permutation of the sheafs which are crossed by the representative circle of the form: that is to say, if we represent the series of sheafs in order by

$$\ldots\ldots\Sigma_{-m},\ \Sigma_{-m+1},\ \ldots\ldots\Sigma_{-1},\ \Sigma_0,\ \Sigma_1,\ \Sigma_2\ldots\ldots\Sigma_n,\ \Sigma_{n+1}\ldots\ldots,$$

they will be changed into

$$\ldots\ldots\Sigma_{-m+h},\ \Sigma_{-m+1+h},\ \ldots\ldots\Sigma_{-1+h},\ \Sigma_h,\ \ldots\ldots\Sigma_{n+h},\ \Sigma_{n+1+h}\ldots\ldots,$$

where h is some integer.

In particular, the fundamental automorph

$$\begin{pmatrix} (T-bU)/\sigma, & -cU/\sigma \\ aU/\sigma, & (T+bU)/\sigma \end{pmatrix}$$

will convert each sheaf into a consecutive sheaf.

The sheafs divide the upper half of the representative circle into an infinite number of equivalent arcs; and the effect of applying the fundamental automorph is to transform each of these into the next following.

Method of Nets.

121. Another useful geometrical method is that of *réseaux*, or nets. Let the plane of reference be divided up into a system of equal and similar parallelograms by means of two sets of equidistant parallel straight lines; such a system will be called a *net*, each of the parallelograms a *mesh*, and each point, where two lines cross, a *node*.

Through any node O draw two rectangular axes OX, OY (fig. 5). Then if $OPRQ$ is a mesh with one vertex at O, and if

$$\varpi_1 = p + qi,$$
$$\varpi_2 = r + si,$$

are the complex quantities corresponding to P and Q, the net is completely defined by ϖ_1, ϖ_2 and may be denoted by (ϖ_1, ϖ_2). The system of nodes is given by

$$z = m\varpi_1 + n\varpi_2,$$

where m, n have all possible integral values, zero included.

The quantity $ps - qr$ measures the area of the parallelogram $OPRQ$: it is called the *norm* of the net, and written $\text{Nm}(\varpi_1, \varpi_2)$.

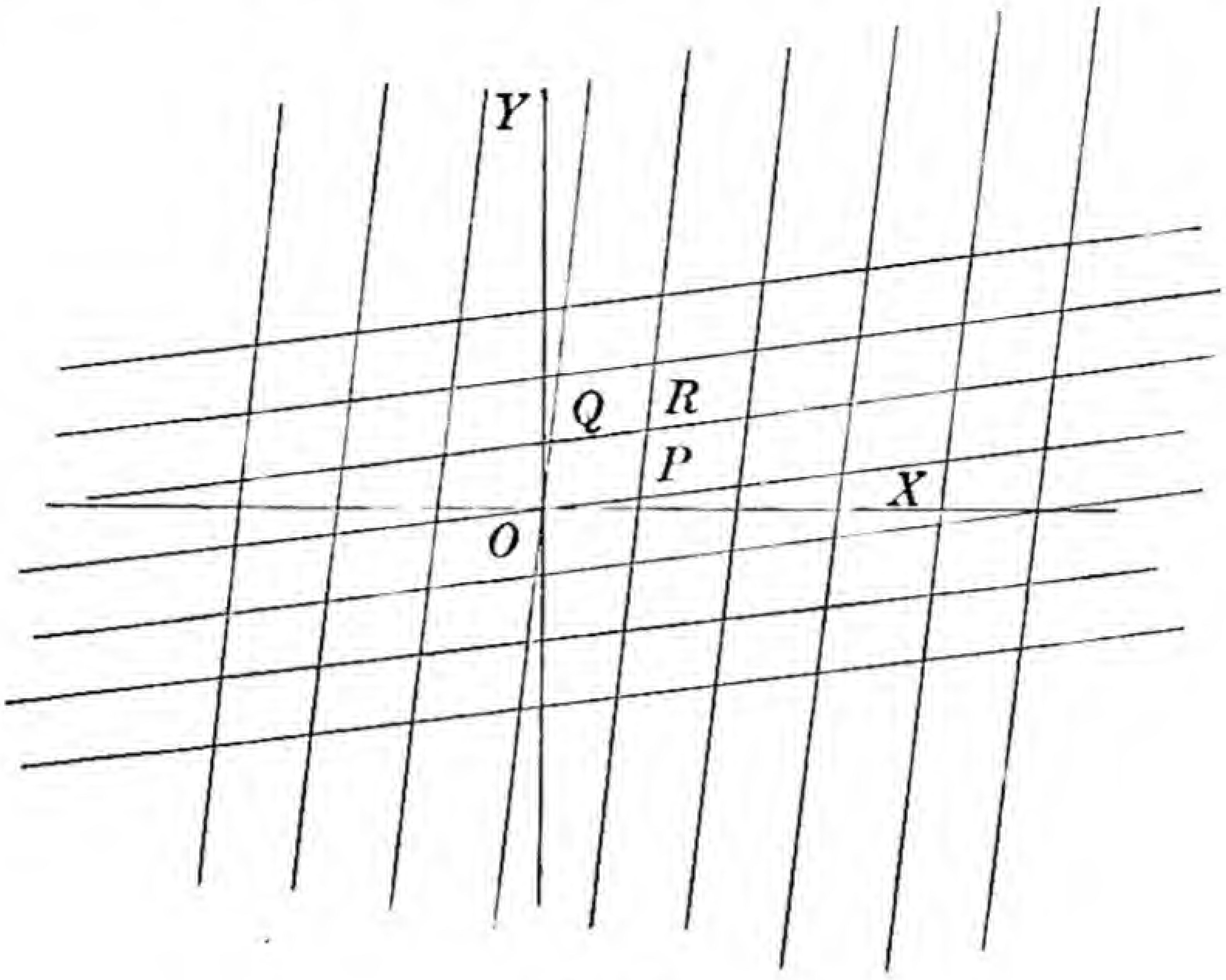

Fig. 5.

Let $\alpha, \beta, \gamma, \delta$ be any integers such that $\alpha\delta - \beta\gamma = 1$: then if

$$\varpi_1' = \alpha\varpi_1 + \gamma\varpi_2,$$
$$\varpi_2' = \beta\varpi_1 + \delta\varpi_2,$$

the net (ϖ_1', ϖ_2') has the same nodal system as (ϖ_1, ϖ_2). Two such nets are said to be properly equivalent, and we may write

$$(\varpi_1', \varpi_2') \backsim (\varpi_1, \varpi_2).$$

More generally, if $\alpha\delta - \beta\gamma = n$, a real integer, all the nodes of (ϖ_1', ϖ_2') will belong to the nodal system of (ϖ_1, ϖ_2) but not conversely; in this case (ϖ_1', ϖ_2') is said to be a multiple of (ϖ_1, ϖ_2).

It is easily verified that

$$\text{Nm}(\varpi_1', \varpi_2') = (\alpha\delta - \beta\gamma) \,.\, \text{Nm}(\varpi_1, \varpi_2),$$

and hence, in particular, if

$$(\varpi_1', \varpi_2') \backsim (\varpi_1, \varpi_2),\ \text{Nm}(\varpi_1', \varpi_2') = \text{Nm}(\varpi_1, \varpi_2).$$

122. Suppose, now, that $f = am^2 + 2bmn + cn^2$ is a definite form of determinant $-\Delta$; then

$$af = (am + bn)^2 + \Delta n^2$$
$$= \text{Nm}\{ma + n(b + i\sqrt{\Delta})\}.$$

This suggests that the form af may be represented by the net $(a, b + i\sqrt{\Delta})$; and in the same way if $f' = a'm^2 + 2b'mn + c'n^2$ is the form into which f is converted by the substitution $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ we may say that af' is represented by the net (ϖ_1, ϖ_2), where

$$\varpi_1 = \alpha a + \gamma(b + i\sqrt{\Delta}),$$
$$\varpi_2 = \beta a + \delta(b + i\sqrt{\Delta}).$$

If s_1, s_2 are the lengths of the sides, and d_1, d_2 the lengths of the diagonals of a mesh of the net (ϖ_1, ϖ_2), we have

$$\begin{aligned} s_1^2 &= (\alpha a + \gamma b)^2 + \gamma^2\Delta = aa', \\ s_2^2 &= (\beta a + \delta b)^2 + \delta^2\Delta = ac', \\ d_1^2 &= (\alpha a + \gamma b + \beta a + \delta b)^2 + (\gamma + \delta)^2\Delta \\ &= a(a' + c' + 2b'), \\ d_2^2 &= a(a' + c' - 2b'). \end{aligned}$$

(Cf. Art. 54.)

123. It is easily proved geometrically that every net is properly equivalent to at least one net of which the mesh is such that neither of its sides is greater than a diagonal.

For suppose that O is any node of the given net; then there will be at least two other nodes which are at a minimum distance from O. Let P be any one of these; then the line OP produced indefinitely both ways will contain an infinite number of nodes. Let this line be moved parallel to itself until it *first* passes through another set of nodes; and let Q be a node on the line in its new position which is at least as near to O as any other node on the new line. Then the parallelogram $OPRQ$, of which OP, OQ are adjacent sides, will be the mesh of a net which contains all the nodes of the given net: moreover, it follows from the way in which P, Q were chosen that $OR \nless OQ \nless OP$, while if RQ is produced to R', so that $QR' = RQ$, R' is a node, and $PQ = OR' \nless OQ$; hence $OPRQ$ satisfies the geometrical conditions above stated.

Such a net will be called a *reduced* net.

With O as origin, let ϖ_1, ϖ_2 be the complex quantities associated with the points P and Q; the conditions of reduction are

$$|\varpi_1| \ngtr |\varpi_1 \pm \varpi_2|,$$
$$|\varpi_2| \ngtr |\varpi_1 \pm \varpi_2|.$$

If (ϖ_1, ϖ_2) is a reduced net, we obtain four associated reduced nets by variation of sign from $(\pm\varpi_1, \pm\varpi_2)$. Of these (ϖ_1, ϖ_2) and

$(\varpi_1, -\varpi_2)$ are improperly equivalent, so that one of this pair must be *properly* equivalent to the given net.

The nets (ϖ_1, ϖ_2), $(-\varpi_1, -\varpi_2)$ may be considered identical; moreover, if (ϖ_1, ϖ_2) is reduced, so also is the equivalent net $(\varpi_2, -\varpi_1)$, hence we may add the further condition $|\varpi_1| \not> |\varpi_2|$.

The corresponding quadratic form af'' satisfies the conditions

$$aa' \not> a(a' \pm 2b' + c'),$$
$$ac' \not> a(a' \pm 2b' + c'),$$
$$aa' \not> ac',$$

or, which is the same thing,

$$|c'| \not< |a'| \not< 2|b'|.$$

These are precisely Lagrange's conditions of reduction; so that the method of nets gives a complete geometrical interpretation of the theory of transformation and reduction as applied to definite forms.

It may be observed that it immediately follows from the geometrical method that if (a, b, c) is a reduced form, a is the numerically least of all the numbers representable by forms of the class to which (a, b, c) belongs, and that if $|c| > |a|$, c is the next least numerically. This may, of course, be proved analytically; and, in fact, it is upon the existence of minimum representable numbers that Hermite has based his general theory of the reduction of definite quadratic forms.

124. It is easy to see that, in general, the geometrical reduction of a net is unique; there are, however, two exceptional cases. The first of these is when there are two nodes P, P' nearer to O than any others, while there are *four* nodes at the next smallest distance. These nodes are the vertices of a rectangle with its centre at O; and if ϖ_1 is the complex quantity corresponding to P, the quantities which define the vertices of the rectangle may be taken to be $\pm\varpi_2$, $\pm(\varpi_2 - \varpi_1)$. There will be two reduced nets properly equivalent to the given one, say

$$(\varpi_1, \varpi_2) \text{ and } (\varpi_1, -\varpi_1 + \varpi_2);$$

the corresponding reduced forms will be of the type $(a, \pm\frac{1}{2}a, c)$ with $|a| < |c|$.

Secondly, there may be *six* nodes, all at the same minimum distance from O. They must evidently be the vertices of a regular hexagon, and the corresponding reduced forms are of the type $(a, \pm \frac{1}{2}a, a)$. Here there are three reduced nets, say (ϖ_1, ϖ_2), $(\varpi_1, -\varpi_1+\varpi_2)$, $(\varpi_2, -\varpi_1+\varpi_2)$ with $\varpi_2 = e^{2\pi i/3}.\varpi_1$, but there are only two reduced forms; the reason being that $(\varpi_2, -\varpi_1+\varpi_2)$ is connected with (ϖ_1, ϖ_2) by the substitution $\begin{pmatrix}0, & -1\\ 1, & 1\end{pmatrix}$, which is an automorphic of $(a, \frac{1}{2}a, a)$.

All this is in agreement with the results of Art. 65.

125. The method of nets may be extended so as to apply to the theory of indefinite forms. We may construct a perfectly consistent algebra of 'hyperbolic' complex quantities $z = x + yj$ upon the lines indicated by the formulæ

$$1.j = j.1 = j, \quad j^2 = 1,$$
$$(x+yj) \pm (x'+y'j) = (x \pm x') + (y \pm y')j,$$
$$(x+yj)(x'+y'j) = (xx'+yy') + (xy'+x'y)j,$$
$$\text{Nm}(x+yj) = x^2 - y^2,$$
$$\arg(x+yj) = \cosh^{-1}\frac{x}{\sqrt{x^2-y^2}} = \sinh^{-1}\frac{y}{\sqrt{x^2-y^2}}.$$

It is easily verified that

$$\text{Nm}(zz') = \text{Nm}(z).\text{Nm}(z'),$$
$$\arg(zz') = \arg z + \arg z'.$$

Following the analogy of the ordinary theory, we represent the quantity $x+yj$ by a point whose rectangular coordinates are (x, y): then the formulæ for addition and subtraction have a geometrical interpretation exactly the same as that for the ordinary theory; and the other formulæ express geometrical relations to the hyperbola $x^2 - y^2 = 1$. Thus if P be the point corresponding to $x+yj$, and if OP meet the hyperbola in P', $\text{Nm}(x+yj) = OP/OP'$, and $\arg(x+yj)$ is twice the numerical measure of the area of the hyperbolic sector OAP', where A is the vertex of the hyperbola on the same branch with P'.

Now if $f = am^2 + 2bmn + cn^2$ is any form with positive determinant D, we have

$$af = (am+bn)^2 - Dn^2$$
$$= \text{Nm}\{ma + n(b + j\sqrt{D})\}.$$

We represent the form af by the net $(a, b+j\sqrt{D})$, and it follows just as above (Art. 122) that if

$$\varpi_1 = \alpha a + \gamma(b+j\sqrt{D}),$$
$$\varpi_2 = \beta a + \delta(b+j\sqrt{D}),$$

the net (ϖ_1, ϖ_2) may be taken to represent af', when f' is derived from f by the substitution $\begin{pmatrix}\alpha, & \beta \\ \gamma, & \delta\end{pmatrix}$.

126. If we draw the lines $x+y=0$, $x-y=0$, it is geometrically evident that the net (ϖ_1, ϖ_2) equivalent to $(a, b+j\sqrt{D})$ can be determined so that the points ϖ_1, ϖ_2 are on opposite sides of one asymptote and on the same side of the other. For suppose that OM is either asymptote: choose any two nodes P, Q, one on each side of OM, and on opposite sides of the other asymptote, and let PQ meet OM in R. Then if the triangle OPQ contains no nodes within it or upon its perimeter (except at O, P, Q), the parallelogram of which OP, OQ are adjacent sides may be taken to form a mesh of the required net: if otherwise, there will be a point P' within or upon the perimeter of OPR and a point Q' within or upon the perimeter of OQR such that $OP'Q'$ is a triangle without any nodes except at O, P', Q', and then if the quantities ϖ_1', ϖ_2' correspond to P', Q', either of the nets (ϖ_1', ϖ_2'), $(\varpi_1', -\varpi_2')$ will have the property required; and one of these must be properly equivalent to the given net.

If we call a net of this kind *reduced*, the analytical condition for a reduced net (ϖ_1, ϖ_2) is that $\text{Nm}(\varpi_1)$ and $\text{Nm}(\varpi_2)$ must have opposite signs. Now with the notation of last Article

$$\text{Nm}(\varpi_1) = aa', \qquad \text{Nm}(\varpi_2) = ac',$$

so that in the form $f' = (a', b', c')$ the coefficients a', c' will have *opposite signs*. A form of this kind may be termed reduced; and it immediately follows (cf. Art. 67) that every form of determinant D is properly equivalent to at least one reduced form, and that the number of reduced forms is finite.

It should be carefully observed, however, that although the number of reduced *forms* is finite, the number of reduced *nets* is infinite. In fact, if (ϖ_1, ϖ_2) is a reduced net, it is geometrically obvious that either $(\varpi_1, \varpi_1+\varpi_2)$ or $(\varpi_1+\varpi_2, \varpi_2)$ is also reduced; and similarly either $(\varpi_1, \varpi_2-\varpi_1)$ or $(\varpi_1-\varpi_2, \varpi_2)$ is reduced. Each reduced net is therefore connected with two adjacent reduced nets by means of one of the substitutions $\begin{pmatrix}1, & 1\\ 0, & 1\end{pmatrix}$, $\begin{pmatrix}1, & 0\\ 1, & 1\end{pmatrix}$ and one of the substitutions $\begin{pmatrix}1, & -1\\ 0, & 1\end{pmatrix}$, $\begin{pmatrix}1, & 0\\ -1, & 1\end{pmatrix}$. In the same way every reduced form is connected with two adjacent reduced forms: for instance $(4, 3, -2)$ is converted into $(8, 1, -2)$ and $(4, -1, -4)$ by the substitutions $\begin{pmatrix}1, & 0\\ 1, & 1\end{pmatrix}$ and $\begin{pmatrix}1, & -1\\ 0, & 1\end{pmatrix}$ respectively.

The infinity of reduced nets belonging to a given class may be arranged into a linear series by means of the above substitutions; the corresponding reduced forms will form a recurring series, and everything proceeds as in the Gaussian theory.

AUTHORITIES.

THE analytical theory of binary quadratic forms contained in Chap. III. is based upon that given by Gauss in Arts. 153—222 of the *Disquisitiones Arithmeticæ:* much help has also been obtained from the 4th section of Dirichlet's *Zahlentheorie*, and Smith's *Report* (1861) Part III. The memoirs of Dirichlet which relate more particularly to this part of the theory are entitled *Démonstration nouvelle d'une proposition relative à la théorie des formes quadratiques* (Liouville, 2nd series, ii. (1857) p. 273), and *Simplification de la théorie des formes binaires du second degré à déterminant positif* (ibid. p. 353 : translated, with additions, from the Berlin memoirs for 1854).

The most important researches anterior to Gauss are those of Lagrange contained in his *Recherches d'Arithmétique* (Nouveaux Mém. de l'Acad. de Berlin 1773, 1775). Lagrange considers forms of the type $Ax^2+Bxy+Cy^2$, and distinguishes them according to the sign of B^2-4AC : he introduces the ideas of transformation and equivalence, and shews that every form is equivalent to one of a limited number of reduced forms. The criteria of reduction are that neither $|A|$ nor $|C|$ is less than $|B|$: for definite forms, this leads to conclusions similar to those in the text, while if $D=B^2-4AC$ is positive, it follows that A, C have opposite signs, and $|B| \not> \sqrt{\frac{1}{5}D}$. Correct classifications are given for a considerable number of special determinants, together with the corresponding forms of linear divisors ; in fact, the memoir abounds in valuable and suggestive matter, and is well worth careful study. Still, the improvements which Gauss effected are undeniable, and he justly claims credit (*D. A.* Art. 222) for the important distinction between proper and improper equivalence.

For the history of the Pellian Equation, see Smith's *Report* (1861) Art. 96. The first rigorous theory of its solution was given by Lagrange: *Solution d'un Problème d'Arithmétique* (Miscell. Taurin. t. iv. (1766—9), or Oeuvres, t. i. p. 671). A list of fundamental solutions of $T^2-DU^2=1$ up to $D=1000$ will be found in Legendre's *Théorie des Nombres.* Degen's *Canon Pellianus* gives also the partial quotients for the recurrent expansion of $\sqrt{D}$.

Many of Euler's memoirs relate to special problems of the theory of quadratic forms: the reader is referred to the analytical table of contents prefixed to the *Comment. Arith.* (t. i. p. lx).

The geometrical method employed in the earlier part of Chap. IV. first arose in connexion with the theory of elliptic modular functions. The best authority on this subject is Klein's *Vorlesungen über die Theorie der elliptischen Modulfunctionen*, edited by R. Fricke, of which the first volume only has yet appeared (Leipzig, 1890). In this work full references are given to the numerous papers on the subject; the part which relates more particularly to quadratic forms will be found on pp. 163—268. According to Klein (l.c. p. 250, note) the first application of the 'Modultheilung' to the theory of indefinite quadratic forms was made by H. J. S. Smith in his paper *Sur les équations modulaires*, written in 1874 and published in the Atti dell' Acc. Reale dei Lincei, t. i. (1877). However, there can be little doubt that the modern development of the modular-function theory dates from Dedekind's letter to Borchardt (Crelle, lxxxiii. (1877), p. 265), and is principally due to the researches of Klein and his school. Special reference should be made to Hurwitz's *Grundlagen einer independenten Theorie der elliptischen Modulfunctionen* (Math. Ann. xviii. p. 528).

On the method of nets, see Gauss's review of Seeber's work on ternary quadratics (Werke, ii. p. 188, or Gött. Anz. July 1831); Dirichlet, *Ueber die Reduction der positiven quadratischen Formen mit drei unbestimmten ganzen Zahlen* (Crelle, xl. (1850), p. 209); Poincaré, *Sur un mode nouveau de représentation géométrique des formes quadratiques définies ou indéfinies* (Journ. de l'École Polyt. cah. 47 (1880), p. 177).

An interesting modification of Gaussian methods is given by Hurwitz: *Ueber eine besondere Art der Kettenbruch-Entwickelung reeller Grössen* (Acta Math. xii. (1889), p. 367).

Hermite's important memoirs on quadratic forms will have to be considered later on: it may be mentioned here that the criteria for a principal reduced form (Art. 117) are enunciated by Hermite in his paper *Sur l'introduction des variables continues dans la théorie des nombres* (Crelle, xli. (1851), p. 207).

CHAPTER V.

Generic Characters of Binary Quadratics.

127. As already explained, the classes of binary quadratic forms belonging to the same determinant D may be arranged into orders, according to the values of $dv(a, b, c)$ and $dv(a, 2b, c)$, where (a, b, c) is any form of the class considered. The classes belonging to each order may be further arranged into groups, each of which constitutes a *genus*. The principle of this distribution depends upon a few simple propositions, the proof of which will now be given.

Let (a, b, c) be a primitive form for which $dv(a, 2b, c) = \sigma$; then it is always possible to assign integers x, y, prime to each other, so that $(ax^2 + 2bxy + cy^2)/\sigma = n$ may be prime to any prescribed number m.

For suppose that $p, p', p''\ldots$ are the different primes which divide a/σ, c/σ and m simultaneously; $q, q', q''\ldots$ those which divide a/σ and m, but not c/σ; $r, r', r''\ldots$ those which divide c/σ and m, but not a/σ; finally, $s, s', s''\ldots$ those which divide m, but not a/σ or c/σ.

Let
$$P = pp'p''\ldots$$
$$Q = qq'q''\ldots$$
$$R = rr'r''\ldots$$
$$S = ss's''\ldots.$$

Since (a, b, c) is primitive, $2b/\sigma$ is prime to P. Now choose x, y so that both are prime to P, x is a multiple of Q, but prime to R, y a multiple of R, but prime to Q, xy a multiple of S, but not divisible by the square of any of the prime factors of S. This may be done in an infinite number of ways and still leave x, y

prime to each other. The simplest way is to put $x = QS'$, $y = RS''$, where $S = S'S''$ is any resolution of S into two factors.

This particular choice of x, y gives

$$n = \frac{ax^2 + 2bxy + cy^2}{\sigma} \equiv \frac{c}{\sigma} \cdot y^2 \pmod{q},$$

$$\equiv \frac{a}{\sigma} \cdot x^2 \pmod{r},$$

$$\equiv \frac{2b}{\sigma} xy \pmod{p},$$

$$\equiv \frac{a}{\sigma} x^2 \text{ or } \frac{c}{\sigma} y^2 \pmod{s},$$

according as y or $x \equiv 0 \pmod{s}$.

Here p, q, r, s denote any prime factors of P, Q, R, S respectively; and it easily follows that n is prime to P, Q, R and S, and therefore also to m.

A special case of this theorem, which is often useful, is that we can always find a number σn capable of primitive representation by (a, b, c) and such that n is prime to $2D$, or, which is the same thing, odd and prime to D.

128. Now suppose that (a, b, c) is a properly primitive form of determinant D, and let n, n' be any two integers prime to $2D$ and capable of primitive representation by (a, b, c). Then if we put

$$n = a\alpha^2 + 2b\alpha\gamma + c\gamma^2,$$

$$n' = a\beta^2 + 2b\beta\delta + c\delta^2,$$

we have identically

$$nn' = x^2 - Dy^2,$$

where

$$x = a\alpha\beta + b(\alpha\delta + \beta\gamma) + c\gamma\delta,$$

$$y = \alpha\delta - \beta\gamma.$$

(Cf. Art. 55.)

From this identity we draw the following six conclusions:—

I. *If p is any odd prime factor of D, $(n|p) = (n'|p)$.*

For since $nn' \equiv x^2 \pmod{p}$, $(nn'|p) = 1$, and therefore

$$(n|p) = (n'|p).$$

II. *If* $D \equiv 3$ (*mod* 4), $(-1)^{\frac{1}{2}(n-1)} = (-1)^{\frac{1}{2}(n'-1)}$.

For $nn' = x^2 - Dy^2 \equiv x^2 + y^2 \pmod{4}$, and since nn' is odd, one of the numbers x, y is odd, and the other even; therefore $nn' \equiv 1 \pmod{4}$, whence $n \equiv n' \pmod{4}$, and

$$(-1)^{\frac{1}{2}(n-1)} = (-1)^{\frac{1}{2}(n'-1)}.$$

III. *If* $D \equiv 2$ (*mod* 8), $(-1)^{\frac{1}{8}(n^2-1)} = (-1)^{\frac{1}{8}(n'^2-1)}$.

We have $nn' \equiv x^2 - 2y^2 \pmod{8}$, and x must be odd, so that $x^2 \equiv 1 \pmod{8}$; also $2y^2 \equiv 2$ or $0 \pmod{8}$: hence $nn' \equiv \pm 1 \pmod{8}$, and therefore $n \equiv \pm n' \pmod{8}$, $n^2 \equiv n'^2 \pmod{16}$, and the theorem follows.

IV. *If* $D \equiv 6$ (*mod* 8), $(-1)^{\frac{1}{2}(n-1)+\frac{1}{8}(n^2-1)} = (-1)^{\frac{1}{2}(n'-1)+\frac{1}{8}(n'^2-1)}$.

Here $nn' \equiv x^2 + 2y^2 \pmod{8}$, and x is odd; so that $nn' \equiv 1$ or $3 \pmod{8}$ according as y is even or odd; therefore $n \equiv n'$ or $3n' \pmod{8}$ respectively, and in each case the truth of the proposition may be verified. This is obvious if $n \equiv n' \pmod{8}$; if $n \equiv 3n' \pmod{8}$, we have

$$\begin{aligned}\tfrac{1}{2}(n-1) + \tfrac{1}{8}(n^2-1) - \tfrac{1}{2}(n'-1) - \tfrac{1}{8}(n'^2-1) &= \tfrac{1}{2}(n-n') + \tfrac{1}{8}(n^2-n'^2)\\ &\equiv n' + n'^2 \pmod{8}\\ &\equiv 0 \pmod{2}.\end{aligned}$$

V. *If* $D \equiv 4$ (*mod* 8), $(-1)^{\frac{1}{2}(n-1)} = (-1)^{\frac{1}{2}(n'-1)}$.

For $nn' \equiv x^2 \equiv 1 \pmod{4}$, and therefore $n \equiv n' \pmod{4}$.

VI. *If* $D \equiv 0$ (*mod* 8), $(-1)^{\frac{1}{2}(n-1)} = (-1)^{\frac{1}{2}(n'-1)}$, *and*

$$(-1)^{\frac{1}{8}(n^2-1)} = (-1)^{\frac{1}{8}(n'^2-1)}.$$

In this case, $nn' \equiv x^2 \equiv 1 \pmod{8}$, and therefore $n \equiv n' \pmod{8}$.

It will be observed that these theorems express properties which are common to all odd numbers, prime to D, representable by the given properly primitive form.

Thus theorem I. states that these numbers are all quadratic residues of p (an odd prime factor of D), or else all non-residues; theorem II. asserts that when $D \equiv 3 \pmod{4}$, the numbers in question are all of the form $4k+1$, or else all of the form $4k+3$; and so on.

129. Let $p, p', p'' \ldots$ be the different odd prime factors of D; and, as above, let n be any odd number prime to D and representable by the properly primitive form (a, b, c). Then it has been proved that the symbols

$$(n|p),\ (n|p'),\ (n|p'')\ldots$$

will have values which may (and in fact do) depend on the form (a, b, c), but not upon the particular value of n. They are called the *quadratic characters* of the form.

Besides these, except when $D \equiv 1 \pmod 4$, there will be one or more *supplementary characters*. Putting, for convenience,

$$(-1)^{\frac{1}{2}(n-1)} = \chi,\ (-1)^{\frac{1}{8}(n^2-1)} = \psi,$$

the supplementary characters are for

$$D \equiv 2, 3, 4, 6, 7, 0 \pmod 8,$$

$$\psi, \chi, \chi, \chi\psi, \chi, \chi \textit{ and } \psi$$

respectively.

The totality of all the particular characters of any form, quadratic and supplementary, makes up its *complete* or *generic* character. Since any number representable by (a, b, c) is representable by any other form of the same class, we may speak of the generic character of a class. Classes which have the same complete character are said to belong to the same genus.

130. The following table, taken from Dirichlet (Crelle, xix. (1839), p. 338), shows in a convenient form the assignable characters of properly primitive classes. In every case, S^2 denotes the largest square which divides D, so that $D = PS^2$ or $2PS^2$ where P is a product of different odd primes p, p', p'', etc.; finally r, r', r'', etc. are the odd prime factors of S which do not divide P. The object of the vertical line which separates the particular characters into two groups will be seen afterwards.

I. $D = PS^2$, $P \equiv 1 \pmod 4$.

$S \equiv 1 \pmod 2$	$(n\mid p), (n\mid p'), \ldots$	$(n\mid r), (n\mid r'), \ldots$
$S \equiv 2 \pmod 4$	$(n\mid p), (n\mid p'), \ldots$	$\chi, (n\mid r), (n\mid r'), \ldots$
$S \equiv 0 \pmod 4$	$(n\mid p), (n\mid p'), \ldots$	$\chi, \psi, (n\mid r), (n\mid r'), \ldots$

II. $D = PS^2$, $P \equiv 3 \pmod 4$.

$S \equiv 1 \pmod 2$	$\chi, (n\mid p), (n\mid p'), \ldots$	$(n\mid r), (n\mid r'), \ldots$
$S \equiv 2 \pmod 4$	$\chi, (n\mid p), (n\mid p'), \ldots$	$(n\mid r), (n\mid r'), \ldots$
$S \equiv 0 \pmod 4$	$\chi, (n\mid p), (n\mid p'), \ldots$	$\psi, (n\mid r), (n\mid r'), \ldots$

III. $D = 2PS^2$, $P \equiv 1 \pmod 4$.

$S \equiv 1 \pmod 2$	$\psi, (n\|p), (n\|p'), \ldots$	$(n\|r), (n\|r'), \ldots$
$S \equiv 0 \pmod 2$	$\psi, (n\|p), (n\|p'), \ldots$	$\chi, (n\|r), (n\|r'), \ldots$

IV. $D = 2PS^2$, $P \equiv 3 \pmod 4$.

$S \equiv 1 \pmod 2$	$\chi\psi, (n\|p), (n\|p'), \ldots$	$(n\|r), (n\|r'), \ldots$
$S \equiv 0 \pmod 2$	$\chi, \psi, (n\|p), (n\|p'), \ldots$	$(n\|r), (n\|r'), \ldots$

131. It should be observed that in order to assign the value of a particular character $(n|p)$ for a given form (a, b, c) it is sufficient to find a number n representable by (a, b, c) and prime to p; and in the same way the supplementary character or characters (if any exist) may be inferred from any odd number representable by the form. Now the extreme coefficients of the form are numbers representable by it; and if (a, b, c) is properly primitive, one or other of the numbers a, c must be prime to any given prime factor of D, and one or other of them must be odd. All the particular characters of a properly primitive form may therefore be determined from its extreme coefficients.

For example, let the form be (6, 3, 13). Here

$$D = -69 = -3 \cdot 23 \equiv 3 \pmod 4,$$

and the particular characters are $(n|3)$, $(n|23)$, and χ. From the coefficient 13, which is odd and prime to 3, we obtain

$$\chi = (-1)^6 = +1,\ (n|3) = (13|3) = +1;$$

and from the coefficient 6, we find

$$(n|23) = (6|23) = (2|23)(3|23) = (+1)(+1) = +1.$$

Therefore the total character of the form is

$$(n|3) = +1,\ (n|23) = +1,\ \chi = +1;$$

or, as Gauss would express it,

$$1, 4;\ R3,\ R23.$$

132. In the case of improperly primitive forms, the characters will be as in the first line of Dirichlet's table, except that n will denote an odd number the double of which is represented by the form. Here again, the total character may be assigned by inspection of the extreme coefficients of the form.

Thus, if the form be $(10, 5, -4)$, for which $D = 65 = 5 \cdot 13$, the particular characters are $(n|5)$ and $(n|13)$. Putting $n=-4/2=-2$, we have $(n|5)=(-2|5)=-1$, $(n|13)=(-2|13)=-1$.

The generic characters of derived forms may be at once inferred from those of the primitive forms from which they are derived.

133. The following tables are given by way of further illustration. For the negative determinants, representatives of the positive primitive classes only have been given. Each line of a table gives the total character of a genus, and representatives of all the classes belonging to that genus. Improperly primitive genera, when they exist, are separated from the rest by a horizontal line. Derived genera are omitted.

$D=-96$.

$(n\|3)$	χ	ψ	
+	+	+	$(1,\ 0,\ 96)$, $(4,\ 2,\ 25)$
−	+	−	$(5,\ 2,\ 20)$, $(5,\ -2,\ 20)$
−	−	−	$(3,\ 0,\ 32)$, $(11,\ 5,\ 11)$
+	−	+	$(7,\ 3,\ 15)$, $(7,\ -3,\ 15)$

$D=-99$.

$(n\|3)$	$(n\|11)$	
+	+	$(1,\ 0,\ 99)$, $(4,\ 1,\ 25)$, $(4,\ -1,\ 25)$
−	+	$(5,\ 1,\ 20)$, $(5,\ -1,\ 20)$, $(9,\ 0,\ 11)$
+	+	$(2,\ 1,\ 50)$
−	+	$(10,\ 1,\ 10)$

$D=136$.

$(n\|17)$	χ	ψ	
+	+	+	$(1,\ 0,\ -136)$, $(-8,\ 0,\ 17)$
+	−	+	$(-1,\ 0,\ 136)$, $(8,\ 0,\ -17)$
−	−	−	$(3,\ 1,\ -45)$, $(3,\ -1,\ -45)$
−	+	−	$(-3,\ 1,\ 45)$, $(-3,\ -1,\ 45)$

$D = 150.$

$(n\|3)$	$(n\|5)$	$\chi\psi$	
$+$	$+$	$+$	$(1, 0, -150)$
$-$	$+$	$-$	$(-1, 0, 150)$
$+$	$-$	$-$	$(3, 0, -50)$
$-$	$-$	$+$	$(-3, 0, 50)$

$D = 185.$

$(n\|5)$	$(n\|37)$	
$+$	$+$	$(1, 0, -185)$
$-$	$-$	$(5, 0, -37)$
$+$	$+$	$(2, 1, -92)$
$-$	$-$	$(10, 5, -16)$

134. The particular characters of the form $(1, 0, -D)$ are all $+1$. This form is called the *principal* form of determinant D, and the class and genus to which it belongs are called the principal class and principal genus.

135. It will be observed that in each of the above examples, the number of complete characters which actually exist is precisely half that which is *a priori* assignable. For instance, when $D = -96$, there are three particular characters $(n|3)$, χ, ψ; and since each may be either $+$ or $-$, the number of complete characters possible *a priori* is 2^3 or 8, whereas only four of these actually occur.

It may be proved by the law of quadratic reciprocity that at least half of the assignable characters of properly primitive classes are impossible. Thus if n is a positive odd number representable by a form f of determinant D, then (Art. 59) D is a quadratic residue of n, and therefore if, in the notation of Dirichlet's table, $D = PS^2$ or $2PS^2$, it follows that P or $2P$, as the case may be, is a quadratic residue of n.

Applying the generalised law of reciprocity (Art. 42), we have in the first case

$$(P|n) = 1,$$

$$(n|P) = (n|P)\,(P|n) = (-1)^{\frac{1}{4}(n-1)(P-1)};$$

that is,

$$(n|p)\,(n|p')\ldots = \chi^{\frac{1}{2}(P-1)}.$$

Therefore if

$$D = PS^2,\ P \equiv 1 \pmod 4,$$

$$(n|p)\,(n|p')\ldots = 1;$$

while if

$$D = PS^2,\ P \equiv 3 \pmod 4,$$

$$\chi\cdot(n|p)\,(n|p')\ldots = 1.$$

On the other hand, if $(2P|n) = 1$, that is, if

$$(-1)^{\frac{1}{8}(n^2-1)}\,(P|n) = 1,$$

we have

$$(n|P) = (-1)^{\frac{1}{8}(n^2-1)}\,.\,(P|n)\,(n|P) = \psi\chi^{\frac{1}{2}(P-1)};$$

hence if

$$D = 2PS^2,\ P \equiv 1 \pmod 4,$$

$$\psi\cdot(n|p)\,(n|p')\ldots = 1;$$

while if

$$D = 2PS^2,\ P \equiv 3 \pmod 4,$$

$$\psi\chi\cdot(n|p)\,(n|p')\ldots = 1.$$

Comparing these results with the table, it appears that in every case the product of all the particular characters in any line of the table which are to the left of the vertical line of division must be equal to $+1$. It is easy to see that this condition excludes precisely one half of the assignable characters.

The theorem that half the assignable characters are impossible will be subsequently proved independently of the law of reciprocity, thus affording a new proof of that law; and it will further be shown that actual genera always exist for the remaining characters, and that each genus of the same order contains the same number of classes.

AUTHORITIES.

Gauss: *Disq. Arith.* Arts. 228—232.

Dirichlet: *Recherches sur diverses applications de l'Analyse infinitésimale à la Théorie des Nombres* (Crelle, xix. (1839), p. 324, or *Werke*, i. p. 413).

See also Dirichlet-Dedekind, *Zahlentheorie*, Supplement IV.; and Smith's *Report*, Art. 98.

CHAPTER VI.

Composition of Forms.

136. LET $$F = AX^2 + 2BXY + CY^2$$ be any binary quadratic form of determinant $D = B^2 - AC$.

Suppose that by means of the bilinear substitution

$$\left.\begin{aligned} X &= p_0xx' + p_1xy' + p_2yx' + p_3yy' \\ Y &= q_0xx' + q_1xy' + q_2yx' + q_3yy' \end{aligned}\right\} \quad \text{............}(1),$$

F becomes ff', where

$$f = ax^2 + 2bxy + cy^2, \quad f' = a'x'^2 + 2b'x'y' + c'y'^2;$$

then we say that F is transformed into ff' by the substitution

$$\begin{pmatrix} p_0, & p_1, & p_2, & p_3 \\ q_0, & q_1, & q_2, & q_3 \end{pmatrix}.$$

In all that follows it will be assumed that the coefficients of the substitution are integral; and we shall write

$$\left.\begin{aligned} P &= p_0q_1 - p_1q_0, & Q &= p_0q_2 - p_2q_0, & R &= p_0q_3 - p_3q_0 \\ S &= p_1q_2 - p_2q_1, & T &= p_1q_3 - p_3q_1, & U &= p_2q_3 - p_3q_2 \end{aligned}\right\} \text{......}(2),$$

where observe that $PU - QT + RS = 0$ identically.

The substitution, or transformation, is said to be primitive, if P, Q, R, S, T, U have no common divisor.

Write $$b^2 - ac = d, \quad b'^2 - a'c' = d';$$

and let M, m, m' be the greatest common divisors of $A, 2B, C$; $a, 2b, c$; $a', 2b', c'$ respectively.

We may regard the equations which define X, Y, as a linear transformation of the single set of variables x, y, by means of which the form $(A, B, C \between x, y)^2$ becomes

$$(f'a, f'b, f'c \between x, y)^2.$$

The determinant of the substitution is

$$\Delta = \begin{vmatrix} p_0x' + p_1y', & p_2x' + p_3y' \\ q_0x' + q_1y', & q_2x' + q_3y' \end{vmatrix} \text{..................}(3)$$

$$= Qx'^2 + (R+S)\,x'y' + Ty'^2,$$

and it follows from the invariant property of the discriminant that

$$(f'b)^2 - (f'a)(f'c) = \Delta^2 . (B^2 - AC),$$

that is,

$$df'^2 = D\Delta^2 \text{ ....}(4).$$

Similarly, putting

$$\Delta' = \begin{vmatrix} p_0x + p_2y, & p_1x + p_3y \\ q_0x + q_2y, & q_1x + q_3y \end{vmatrix} \text{..................}(5)$$

$$= Px^2 + (R-S)\,xy + Uy^2,$$

we have

$$d'f^2 = D\Delta'^2 \text{.........................}(6).$$

Let

$$\delta = dv\,(Q,\ R+S,\ T),$$

$$\delta' = dv\,(P,\ R-S,\ U);$$

then evidently, by (4) and (6),

$$dm'^2 = D\delta^2, \quad d'm^2 = D\delta'^2.$$

Again let

$$k = dv\,(P,\ Q,\ R,\ S,\ T,\ U);$$

then it can be easily proved that

$$k = dv\,(\delta,\ \delta').$$

For suppose $dv\,(\delta, \delta') = \mu$: then μ divides P, Q, T, U, $2R$, $2S$, and therefore either $k = \mu$ or $k = \frac{1}{2}\mu$. In the latter case μ must be even, P/k, Q/k, T/k, U/k must all be even, and R/k, S/k both odd. But this is inconsistent with the identity

$$\frac{R}{k} \cdot \frac{S}{k} = \frac{Q}{k} \cdot \frac{T}{k} - \frac{P}{k} \cdot \frac{U}{k}:$$

therefore

$$k = \mu = dv\,(\delta,\ \delta').$$

Hence

$$Dk^2 = dv\,(D\delta^2,\ D\delta'^2)$$

$$= dv\,(dm'^2,\ d'm^2) \text{ ....}(7).$$

It is clear that d/D, d'/D are rational squares; so that putting

$$d/D = n^2, \quad d'/D = n'^2 \text{ ....}(8),$$

n, n' will be rational.

It has been proved that

$$\Delta^2 = n^2 f'^2, \quad \Delta'^2 = n'^2 f^2,$$

we can therefore choose the signs of n, n', so that

$$\Delta = nf', \quad \Delta' = n'f;$$

having done this, we find by comparison of coefficients

$$\left.\begin{aligned} \frac{P}{a} &= \frac{R-S}{2b} = \frac{U}{c} = n' \\ \frac{Q}{a'} &= \frac{R+S}{2b'} = \frac{T}{c'} = n \end{aligned}\right\} \dots\dots\dots\dots\dots\dots\dots(9).$$

The form f is said to be taken directly or inversely, according as n is positive or negative: and similarly for f', n'.

It may be verified that

$$\Delta\Delta' = (q_1q_2 - q_0q_3)X^2 + (p_0q_3 + p_3q_0 - p_1q_2 - p_2q_1)XY$$
$$+ (p_1p_2 - p_0p_3)Y^2 \dots\dots\dots(10)$$

identically; and comparing this with

$$\Delta\Delta' = nf' \,.\, n'f = nn'F,$$

we infer that

$$\frac{q_1q_2 - q_0q_3}{A} = \frac{p_0q_3 + p_3q_0 - p_1q_2 - p_2q_1}{2B} = \frac{p_1p_2 - p_0p_3}{C} = nn' \dots(11).$$

Conversely, if the nine equations

$$\left.\begin{gathered} P = an', \quad R - S = 2bn', \quad U = cn' \\ Q = a'n, \quad R + S = 2b'n, \quad T = c'n \\ q_1q_2 - q_0q_3 = Ann', \quad p_0q_3 + p_3q_0 - p_1q_2 - p_2q_1 = 2Bnn', \\ p_1p_2 - p_0p_3 = Cnn' \end{gathered}\right\} \dots(\Omega)$$

are satisfied, then the substitution $\begin{pmatrix} p_0, & p_1, & p_2, & p_3 \\ q_0, & q_1, & q_2, & q_3 \end{pmatrix}$ will transform F into ff'.

Gauss obtains the system (Ω) by direct comparison of the coefficients in the identity

$$(A, B, C \between X, Y)^2 = (a, b, c \between x, y)^2 \times (a', b', c' \between x', y')^2:$$

this leads to nine equations such as

$$Ap_0^2 + 2Bp_0q_0 + Cq_0^2 = aa',$$
$$Ap_0p_1 + B(p_0q_1 + p_1q_0) + Cq_0q_1 = ab',$$

and so on: from these the equivalent set (Ω) is derived (see *D. A.* Art. 235). The simplified method here adopted is due to H. J. S. Smith (*Report*, Arts. 106, 107).

137. It follows from the identity

$$AX^2 + 2BXY + CY^2 = (ax^2 + 2bxy + cy^2)(a'x'^2 + 2b'x'y' + c'y'^2)$$

that M divides mm'. It can be shewn that mm' divides Mk^2.

For by equating the coefficients of x^2, xy, y^2 in the above identity, we obtain

$$\left.\begin{aligned} af' &= A\left(\frac{\partial X}{\partial x}\right)^2 + 2B\left(\frac{\partial X}{\partial x}\right)\left(\frac{\partial Y}{\partial x}\right) + C\left(\frac{\partial Y}{\partial x}\right)^2 \\ 2bf' &= 2A\frac{\partial X}{\partial x}\cdot\frac{\partial X}{\partial y} + 2B\left(\frac{\partial X}{\partial x}\cdot\frac{\partial Y}{\partial y} + \frac{\partial X}{\partial y}\cdot\frac{\partial Y}{\partial x}\right) + 2C\frac{\partial Y}{\partial x}\cdot\frac{\partial Y}{\partial y} \\ cf' &= A\left(\frac{\partial X}{\partial y}\right)^2 + 2B\frac{\partial X}{\partial y}\cdot\frac{\partial Y}{\partial y} + C\left(\frac{\partial Y}{\partial y}\right)^2 \end{aligned}\right\}\dots(12).$$

Multiply, in order, by

$$\left(\frac{\partial Y}{\partial y}\right)^2, \quad -\frac{\partial Y}{\partial x}\cdot\frac{\partial Y}{\partial y}, \quad \left(\frac{\partial Y}{\partial x}\right)^2,$$

and add; thus

$$A\left(\frac{\partial X}{\partial x}\cdot\frac{\partial Y}{\partial y} - \frac{\partial X}{\partial y}\cdot\frac{\partial Y}{\partial x}\right)^2 = \left\{a\left(\frac{\partial Y}{\partial y}\right)^2 - 2b\frac{\partial Y}{\partial x}\cdot\frac{\partial Y}{\partial y} + c\left(\frac{\partial Y}{\partial x}\right)^2\right\}f'.$$

Every term on the right-hand is divisible by mm': hence the expression on the left, that is $A\Delta^2$, is divisible by mm'. In the same way we can prove that $2B\Delta^2$, $C\Delta^2$ are each divisible by mm': and therefore mm' divides $M\delta^2$. Similarly mm' divides $M\delta'^2$: and hence finally $Mk^2 = dv\,(M\delta^2, M\delta'^2)$ is divisible by mm'.

Again let

$$\mathfrak{M} = dv\,(A, B, C), \quad \mathfrak{m} = dv\,(a, b, c), \quad \mathfrak{m}' = dv\,(a', b', c');$$

then it can be proved in precisely the same way that $\mathfrak{m}\mathfrak{m}'$ divides $\mathfrak{M}k^2$.

It will now be supposed that $k = 1$, so that the transformation is primitive. When this is the case, F is said to be *compounded* of f and f'.

It follows from what has been already proved that in the case of composition

$$\left.\begin{aligned} D &= dv\,(dm'^2,\ d'm^2) \\ M &= mm', \quad \mathfrak{M} \equiv 0 \pmod{\mathfrak{m}\mathfrak{m}'} \end{aligned}\right\}\dots\dots\dots\dots(13),$$

and also that

$$mn' = \sqrt{d'm^2/D}, \text{ and } m'n = \sqrt{dm'^2/D}$$

will be integers and relatively prime.

The second of equations (12) shews that $\mathfrak{M}$ divides $\mathfrak{m}m'$: and in the same way it divides $\mathfrak{m}'m$: hence if $\mathfrak{m} = m$ and $\mathfrak{m}' = m'$, that is, if f, f' are both properly primitive or derived from properly primitive forms, F is properly primitive, or derived from a properly primitive form; whereas in any other case $\mathfrak{M} = \frac{1}{2}mm' = \frac{1}{2}M$, and

F is improperly primitive or derived from an improperly primitive form.

138. We are now confronted by the fundamental problem:—

Given two forms (a, b, c), (a', b', c'), to find, when possible, a form (A, B, C) compounded of them, each component form being taken in a prescribed way.

In order that a solution may be possible, the ratio of the determinants of the given forms must be a rational square. Suppose this to be the case; let d, d', m, m' have the same meanings as before, and let $D = dv(dm'^2, d'm^2)$ taken with the same sign as d, d'.

Let
$$n = \sqrt{d/D}, \quad n' = \sqrt{d'/D},$$
the sign of each being taken positive or negative according as the corresponding form f or f' is to be taken directly or inversely. Then n, n' are rational, and mn', $m'n$ are integers and relatively prime.

Hence by the first six of equations (Ω), P, Q, R, S, T, U are determined: and it is easily seen that they are all integral and relatively prime, so that $k = 1$.

The next step is to find eight integers $p_0, p_1, p_2, p_3, q_0, q_1, q_2, q_3$ so as to give P, Q, R, S, T, U these known values.

Consider the skew-symmetrical system of equations
$$\begin{aligned}
& x_1 U - x_2 T + x_3 S = 0 \\
-\, x_0 U \quad & + x_2 R - x_3 Q = 0 \\
x_0 T - x_1 R \quad & + x_3 P = 0 \\
-\, x_0 S + x_1 Q - x_2 P \quad & = 0:
\end{aligned}$$
these are equivalent to *two* independent relations; for if we multiply the first three equations in order by R, T, U respectively and add, we are led to the identity
$$x_3 (PU - QT + RS) = 0;$$
and similarly for any other group of three.

Now let $\theta_0, \theta_1, \theta_2, \theta_3$ be any multipliers whatever, and put
$$\begin{aligned}
\eta_0 &= \qquad\qquad \theta_1 P + \theta_2 Q + \theta_3 R, \\
\eta_1 &= -\theta_0 P \qquad\quad + \theta_2 S + \theta_3 T, \\
\eta_2 &= -\theta_0 Q - \theta_1 S \qquad\quad + \theta_3 U, \\
\eta_3 &= -\theta_0 R - \theta_1 T - \theta_2 U,
\end{aligned}$$

then the preceding set of equations may be satisfied (and in the most general manner) by putting

$$x_0 : x_1 : x_2 : x_3 = \eta_0 : \eta_1 : \eta_2 : \eta_3.$$

We may suppose $\theta_0, \theta_1, \theta_2, \theta_3$ to be rational, or indeed integral, and chosen so that $\eta_0 \ldots \eta_3$ do not all vanish; and then we may suppose x_0, x_1, x_2, x_3 to have *integral* values proportional to

$$\eta_0, \eta_1, \eta_2, \eta_3.$$

Call these values q_0, q_1, q_2, q_3; we may take them so as to have no common divisor, and therefore we can determine four integers $\pi_0, \pi_1, \pi_2, \pi_3$, such that

$$\pi_0 q_0 + \pi_1 q_1 + \pi_2 q_2 + \pi_3 q_3 = 1.$$

Further, let p_0, p_1, p_2, p_3 be the values of $\eta_0, \eta_1, \eta_2, \eta_3$ when

$$\theta_0, \theta_1, \theta_2, \theta_3 = \pi_0, \pi_1, \pi_2, \pi_3;$$

then $p_0, p_1, p_2, p_3, q_0, q_1, q_2, q_3$ will be a set of eight integers such as is required.

We have in fact

$$\begin{aligned} p_0 q_1 - p_1 q_0 &= (\pi_1 P + \pi_2 Q + \pi_3 R)\, q_1 + (\pi_0 P - \pi_2 S - \pi_3 T)\, q_2 \\ &= (\pi_0 q_0 + \pi_1 q_1 + \pi_2 q_2 + \pi_3 q_3)\, P \\ &\quad + \pi_2 (-q_0 S + q_1 Q - q_2 P) \\ &\quad + \pi_3 (-q_0 T + q_1 R - q_3 P) \\ &= P, \end{aligned}$$

since $$\pi_0 q_0 + \pi_1 q_1 + \pi_2 q_2 + \pi_3 q_3 = 1,$$

and the coefficients of π_2, π_3 in the other terms vanish.

This is one of the equations which have to be satisfied: and the rest may be verified in a similar way.

It remains to be proved that the values of A, B, C derived from the last three of equations (Ω) are integral. Returning to the identity

$$\{Px^2 + (R - S)\, xy + Uy^2\}\, \{Qx'^2 + (R + S)\, x'y' + Ty'^2\} \\ = nn'(AX^2 + 2BXY + CY^2),$$

and remembering the meaning of δ, δ', we see that if $(R + S)/\delta$ and $(R - S)/\delta'$ are both even, $2Ann'$, $2Bnn'$, $2Cnn'$ are divisible by $2\delta\delta'$.

Now $D\delta^2 = dm'^2$, and therefore $\delta^2 = m'^2 n^2$: similarly $\delta'^2 = m^2 n'^2$, and $\delta\delta'/nn' = \pm\, mm' =$ an integer. If, then, as in the case now considered $Ann'/\delta\delta' = \pm A/mm'$ is an integer, *a fortiori* A is an integer, and similarly B, C are integers.

On the other hand, if either $(R+S)/\delta$ or $(R-S)/\delta'$ be odd, then either $2b/m$ or $2b'/m'$ is odd, and hence either m or m' is even: $2Ann'$, $2Bnn'$, $2Cnn'$ are divisible by $\delta\delta'$, the quotients (neglecting sign) being

$$2A/mm', \quad 2B/mm', \quad 2C/mm';$$

and since $mm'/2$ is an integer, we conclude, as before, that A, B, C are integers.

139. It will be observed that a form F compounded of f, f' in a prescribed manner may be found in an infinite number of ways: but it can be shewn that all such forms are properly equivalent.

For suppose $F = (A, B, C)$ and $F' = (A', B', C')$ to be any two such forms, and let

$$\begin{pmatrix} p_0, & p_1, & p_2, & p_3 \\ q_0, & q_1, & q_2, & q_3 \end{pmatrix}, \quad \begin{pmatrix} p_0', & p_1', & p_2', & p_3' \\ q_0', & q_1', & q_2', & q_3' \end{pmatrix}$$

be two primitive substitutions which transform F, F' respectively into ff'.

Then $$p_0'q_1' - p_1'q_0' = p_0q_1 - p_1q_0 = an';$$

and similarly for any other corresponding pair of determinants.

Now let integers (01), (02), (12), etc. be chosen so that

$$(01)(p_0q_1 - p_1q_0) + (02)(p_0q_2 - p_2q_0) + \dots = 1,$$

or say $$\Sigma(\lambda, \mu)(p_\lambda q_\mu - p_\mu q_\lambda) = 1:$$

and put

$$\Sigma(\lambda, \mu)(p_\lambda' q_\mu - p_\mu' q_\lambda) = \alpha,$$
$$\Sigma(\lambda, \mu)(p_\lambda p_\mu' - p_\mu p_\lambda') = \beta,$$
$$\Sigma(\lambda, \mu)(q_\lambda' q_\mu - q_\mu' q_\lambda) = \gamma,$$
$$\Sigma(\lambda, \mu)(p_\lambda q_\mu' - p_\mu q_\lambda') = \delta.$$

Then if ν is any one of the numbers 0, 1, 2, 3,

$$\begin{aligned} \alpha p_\nu + \beta q_\nu &= \Sigma(\lambda, \mu)\{p_\nu(p_\lambda' q_\mu - p_\mu' q_\lambda) + q_\nu(p_\lambda p_\mu' - p_\mu p_\lambda')\} \\ &= \Sigma(\lambda, \mu)\{p_\lambda'(p_\nu q_\mu - p_\mu q_\nu) - p_\mu'(p_\nu q_\lambda - p_\lambda q_\nu)\} \\ &= \Sigma(\lambda, \mu)\{p_\lambda'(p_\nu' q_\mu' - p_\mu' q_\nu') - p_\mu'(p_\nu' q_\lambda' - p_\lambda' q_\nu')\} \\ &= \Sigma(\lambda, \mu) p_\nu'(p_\lambda' q_\mu' - p_\mu' q_\lambda') \\ &= p_\nu' \Sigma(\lambda, \mu)(p_\lambda q_\mu - p_\mu q_\lambda) \\ &= p_\nu'. \end{aligned}$$

Similarly $$\gamma p_\nu + \delta q_\nu = q_\nu';$$
and hence
$$\begin{vmatrix} p_\lambda', & p_\mu' \\ q_\lambda', & q_\mu' \end{vmatrix} = \begin{vmatrix} \alpha p_\lambda + \beta q_\lambda, & \alpha p_\mu + \beta q_\mu \\ \gamma p_\lambda + \delta q_\lambda, & \gamma p_\mu + \delta q_\mu \end{vmatrix}$$
$$= (\alpha\delta - \beta\gamma)(p_\lambda q_\mu - p_\mu q_\lambda):$$
therefore $$\alpha\delta - \beta\gamma = 1.$$

Now if X, Y are the variables of F, and X', Y' those of F',
$$X' = p_0'xx' + p_1'xy' + p_2'x'y + p_3'yy'$$
$$= (\alpha p_0 + \beta q_0)xx' + \ldots$$
$$= \alpha X + \beta Y,$$
and similarly $$Y' = \gamma X + \delta Y;$$
from which it is clear that F is transformed into F' by the proper substitution $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$, so that F, F' are equivalent.

It is obvious that, conversely, if F is compounded of f, f' and F' is properly equivalent to F, then F' is also compounded of f, f' in the same way as F is.

More generally, if F' is transformable into ff', but not necessarily compounded of f and f', and if, as before, F is compounded of f, f', then F' contains F.

For with the same notation as before, we shall have
$$p_0'q_1' - p_1'q_0' = k(p_0q_1 - p_1q_0), \text{ etc.},$$
and it can be shewn that, as before,
$$p_\nu' = \alpha p_\nu + \beta q_\nu, \quad q_\nu' = \gamma p_\nu = \delta q_\nu,$$
$$p_\lambda'q_\mu' - p_\mu'q_\lambda' = (\alpha\delta - \beta\gamma)(p_\lambda q_\mu - p_\mu q_\lambda):$$
hence $$\alpha\delta - \beta\gamma = k,$$
and F' is transformed into F by the transformation $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$ of determinant k: that is, F is contained in F'.

Many of the succeeding propositions may be generalised in the same way.

140. Let f be transformed into an equivalent form ϕ by the substitution $\begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix}$; then it is clear that F is transformed into $\phi f'$ by the substitution
$$X = (p_0x' + p_1y')(\alpha x + \beta y) + (p_2x' + p_3y')(\gamma x + \delta y),$$
$$Y = (p_0x' + q_1y')(\alpha x + \beta y) + (q_2x' + q_3y')(\gamma x + \delta y),$$
that is,
$$\begin{pmatrix} \alpha p_0 + \gamma p_2, & \alpha p_1 + \gamma p_3, & \beta p_0 + \delta p_2, & \beta p_1 + \delta p_3 \\ \alpha q_0 + \gamma q_2, & \alpha q_1 + \gamma q_3, & \beta q_0 + \delta q_2, & \beta q_1 + \delta q_3 \end{pmatrix}.$$

Let the determinants of this matrix be called

$$P', Q', R', S', T', U',$$

and let

$$\phi = (a'', b'', c'').$$

Then we find by direct calculation

$$\begin{aligned} P' &= \alpha^2 P + \alpha\gamma (R - S) + \gamma^2 U \\ &= n' (a\alpha^2 + 2b\alpha\gamma + c\gamma^2) = a''n'; \end{aligned}$$

and similarly

$$R' - S' = 2b''n',$$
$$U' = c''n'.$$

Again,

$$Q' = (\alpha\delta - \beta\gamma) Q = (\alpha\delta - \beta\gamma) a'n,$$

and so

$$R' + S' = 2 (\alpha\delta - \beta\gamma) b'n,$$
$$T' = (\alpha\delta - \beta\gamma) c'n.$$

Finally,

$$\begin{aligned} (\alpha q_1 + \gamma q_3) (\beta q_0 + \delta q_2) - (\alpha q_0 + \gamma q_2) (\beta q_1 + \delta q_3) \\ = (\alpha\delta - \beta\gamma) (q_1 q_2 - q_0 q_3) \\ = (\alpha\delta - \beta\gamma) Ann'; \end{aligned}$$

and similarly the other two corresponding expressions formed as in the last three of equations (Ω) reduce to

$$2 (\alpha\delta - \beta\gamma) Bnn', \quad (\alpha\delta - \beta\gamma) Cnn'$$

respectively.

Now if ϕ is properly equivalent to f, $\alpha\delta - \beta\gamma = 1$, and we conclude that F is compounded of ϕ, f' in the same way as it is compounded of f and f'. If, on the other hand, $\alpha\delta - \beta\gamma = -1$, so that ϕ is improperly equivalent to f, F is still compounded of ϕ and f', but n has to be taken with a different sign; that is, ϕ has to be taken inversely or directly according as f was taken directly or inversely.

It follows that in all problems of composition we may substitute for any form, taken inversely, an improperly equivalent form, for example its opposite, taken directly. In future, unless the contrary is expressly stated, it will be supposed that all forms which are compounded are taken directly.

141. It is now evident that we may speak of the composition of *classes*; namely, if f, f' are any two forms belonging to classes K, K', then any form F compounded of them will belong to a perfectly determinate class, which may be said to be compounded of K, K' and denoted by KK'.

It is clear that the symbols $K'K$, KK' mean the same thing, because, in compounding two forms, the process has been symmetrical with respect to the components.

A class can always be compounded with itself: this process is called *duplication*, and the class resulting from the duplication of K is denoted by K^2.

142. The composition of forms may be treated in another, and in some respects a simpler way, which is due to F. Arndt[1].

Let f, f', d, d', m, m' have the same meanings as before; let

$$D = dv\,(dm'^2, d'm^2), \quad n = \sqrt{d/D}, \quad n' = \sqrt{d'/D}.$$

Then we see, as before, that mn' and $m'n$ are integers and relatively prime.

Now suppose that *by definition*

$$P = an', \quad Q = a'n, \quad R = b'n + bn',$$
$$U = cn', \quad T = c'n, \quad S = b'n - bn':$$

then it follows from the definitions that P, Q, R, S, T, U are all integers and relatively prime.

Let $\mu = dv\,(P, Q, R)$; then we can prove the following propositions:—

(i) The integers ab', $a'b$, $bb' + Dnn'$, are all divisible by μ.

(Observe that $Dnn' = \sqrt{dd'}$, and is therefore an integer, since, by supposition, d/d' is a rational square.)

We have

$$ab' . mn' = b'mP, \qquad ab' . m'n = m'(aR - bP),$$
$$a'b . m'n = bm'Q, \qquad a'b . mn' = m\,(a'R - b'Q),$$
$$(bb' + Dnn')\,mn' = m\,(b'R - c'Q), \quad (bb' + Dnn')\,m'n = m'\,(bR - cP).$$

Now all the expressions on the right-hand of these equations are divisible by μ: and since mn', $m'n$ are prime to each other, the truth of the proposition is evident.

(ii) In the next place, aa' is divisible by μ^2.

Since $\quad aa' . mn' = a'mP$, and $aa' . m'n = am'Q$,

we see that aa' is divisible by μ. Hence $aa'P$, $aa'Q$, $aa'R$ are all divisible by μ^2.

[1] Crelle, t. 56, p. 64 (1859).

Again
$$aa'S = ab'Q - a'bP,$$
$$aa'T = ab'R - (bb' + Dnn')P,$$
$$aa'U = a'bR - (bb' + Dnn')Q.$$

Hence, and from (i), we infer that $aa'S$, $aa'T$, $aa'U$ are all divisible by μ^2; and since P, Q, R, S, T, U have no common divisor, it follows that aa' is divisible by μ^2.

(iii) Let $aa'/\mu^2 = A$: then an integer B can be found so as to satisfy simultaneously the three congruences

$$\left.\begin{aligned} \frac{P}{\mu}.B &\equiv \frac{ab'}{\mu} \\ \frac{Q}{\mu}.B &\equiv \frac{a'b}{\mu} \\ \frac{R}{\mu}.B &\equiv \frac{bb' + Dnn'}{\mu} \end{aligned}\right\} \pmod{A}.$$

Choosing integers α, β, γ so that
$$\alpha P + \beta Q + \gamma R = \mu,$$
let us put
$$B = \frac{ab'}{\mu}.\alpha + \frac{a'b}{\mu}.\beta + \frac{bb' + Dnn'}{\mu}\gamma;$$
then it may be verified that this value does in fact satisfy all the congruences.

For we have
$$\begin{aligned} \mu(PB - ab') &= P\{ab'\alpha + a'b\beta + (bb' + Dnn')\gamma\} - \mu ab' \\ &= ab'(\mu - \beta Q - \gamma R) - \mu ab' \\ &\quad + P\{a'b\beta + (bb' + Dnn')\gamma\} \\ &= \beta\{a'bP - ab'Q\} + \gamma\{(bb' + Dnn')P - ab'R\}. \end{aligned}$$

Substituting for P, Q, R their values, and writing $(b'^2 - a'c')$ for Dn'^2, this reduces to
$$\{\beta(bn' - b'n) - \gamma c'n\}aa',$$
that is, to
$$-(\beta S + \gamma T)aa'.$$
Hence
$$\mu(PB - ab') \equiv 0 \pmod{aa'};$$
and therefore
$$\frac{P}{\mu}.B - \frac{ab'}{\mu} \equiv 0 \pmod{A}.$$

It may be similarly verified that the other congruences are satisfied: in fact
$$\mu(QB - a'b) = (\alpha S + \gamma U)aa',$$
$$\mu\{RB - (bb' + Dnn')\} = (\alpha T + \beta Q)aa'.$$

Since P/μ, Q/μ, R/μ are relative primes, it follows that all values of B which satisfy the three congruences simultaneously, are congruous (mod A).

After some easy reduction, we find that

$$\mu^2(B^2 - D) = aa'\{ac'\alpha^2 + a'c\beta^2 + cc'\gamma^2 + 2b'c\beta\gamma + 2bc'\gamma\alpha + 2(bb' - Dnn')\alpha\beta\},$$

whence

$$B^2 - D \equiv 0 \pmod{A}.$$

Putting $\dfrac{B^2 - D}{A} = C$, the form (A, B, C) will be of determinant D, and it can be shewn to be compounded of (a, b, c) and (a', b', c').

In fact, if we put

$$X = \mu xx' + \frac{\mu(b' - Bn')}{a'} xy' + \frac{\mu(b - Bn)}{a} x'y + \mu \, . \, \frac{bb' + Dnn' - B(bn' + b'n)}{aa'} yy',$$

$$Y = \frac{an'}{\mu} xy' + \frac{a'n}{\mu} x'y + \frac{bn' + b'n}{\mu} yy',$$

all the coefficients of the substitution are integral, and we have identically

$$\frac{1}{\mu}(ax + by + ny\sqrt{D})(a'x' + b'y' + n'y'\sqrt{D}) = AX + BY + Y\sqrt{D},$$

with a similar identity obtained by changing the sign of $\sqrt{D}$ throughout.

Multiplying these together, we obtain

$$\frac{1}{\mu^2} \, . \, af \, . \, a'f' = AF,$$

and therefore, since

$$A = aa'/\mu^2,$$

$$F = ff';$$

that is, F is transformable into ff'.

It is easily proved that the six determinants of the transformation are P, Q, R, S, T, U: hence the substitution is primitive, and F is compounded of f and f'.

In every case, then, where composition is possible, we can compound (a, b, c), (a', b', c') into (A, B, C), where

$$A = aa'/\mu^2,$$

$$\left.\begin{aligned} \frac{an'}{\mu}\cdot B &\equiv \frac{ab'}{\mu} \\ \frac{a'n}{\mu} B &\equiv \frac{a'b}{\mu} \\ \frac{b'n+bn'}{\mu} B &\equiv \frac{bb'+Dnn'}{\mu} \end{aligned}\right\} \text{(mod A)},$$

$$C=(B^2-D)/A.$$

Here $$D=dv\,(dm'^2,\ d'm^2);$$
$$n=\sqrt{d/D},\quad n'=\sqrt{d'/D};$$
$$\mu=dv\,(an',\ a'n,\ b'n+bn').$$

143. Suppose that K, K', K'' are three classes the determinants of which are in the proportion of three square numbers: and let f, f', f'' be any three forms belonging to them. Then by compounding f and f' we get a form of the class KK', and by compounding this with f'', we get a form belonging to the class $(KK')\,K''$. If we first compound f' with f'', and then the result with f, we get a form of the class $K\,(K'K'')$.

It will now be shewn that the two forms obtained by these different processes are equivalent, or, which is the same thing, that the classes $(KK')\,K''$ and $K\,(K'K'')$ are identical.

Let (a, b, c), (a', b', c'), (a'', b'', c'') be the forms f, f', f''; d, d', d'' their determinants, and so on; the notation being as before, with the addition of corresponding symbols for f''.

Then by Arndt's process we may compound f, f' into (A, B, C), or F say, where $A=aa'/\mu^2$, etc. as above. The determinant of F is $D=dv\,(dm'^2,\ d'm^2)$; and $M=dv\,(A,\ 2B,\ C)=mm'$.

By the same process let us compound F and f'' into a form $\Phi=(\Lambda,\ \mathrm{B},\ \Gamma)$.

Let Δ be the determinant of Φ.

Then $$\Delta=dv\,(Dm''^2,\ d''M^2).$$

Now since $$D=dv\,(dm'^2,\ d'm^2),$$
$$Dm''^2=dv\,(dm'^2m''^2,\ d'm''^2m^2):$$

also $$d''M^2=d''m^2m'^2:$$

therefore $$\Delta=dv\,(dm'^2m''^2,\ d'm''^2m^2,\ d''m^2m'^2).$$

Let us write $\nu=\sqrt{d/\Delta}$, $\nu'=\sqrt{d'/\Delta}$, $\nu''=\sqrt{d''/\Delta}$: these quantities are all rational: and moreover $m'm''\nu$, $m''m\nu'$, $mm'\nu''$ are all integers, and relatively prime.

Further, let $N = \sqrt{D/\Delta} = \nu/n = \nu'/n'$.

We have $\mathrm{A} = Aa''/\mu'^2 = aa'a''/\mu^2\mu'^2$,

where $\mu' = dv\,(A\nu'',\ a''N,\ Nb'' + \nu''B)$.

Now $\mu = dv\,(an',\ a'n,\ nb' + n'b)$,

and therefore $\mu\mu'$ divides the following integers:

$$\mu \,.\, A\nu'' = aa'\nu'',$$
$$an' \,.\, a''N = a''a\nu',$$
$$a'n \,.\, a''N = a'a''\nu,$$
$$(nb' + n'b) \,.\, a''N = a''\,(\nu b' + \nu' b).$$

Again, since $an'B \equiv ab' \pmod{\mu A}$,

therefore $an'\,(Nb'' + \nu''B) \equiv a\,(\nu'b'' + \nu''b') \pmod{\mu A\nu''}$.

Hence we see that $\mu\mu'$ divides $a\,(\nu'b'' + \nu''b')$; and similarly it divides $a'\,(\nu''b + \nu b'')$.

Finally, since $(b'n + bn')B \equiv bb' + Dnn'$

$$\equiv bb' + \Delta\nu\nu' \pmod{\mu A},$$

we have

$$(Nb'' + \nu''B)\,(b'n + bn') \equiv \nu b'b'' + \nu'b''b + \nu''bb' + \Delta\nu\nu'\nu'' \pmod{\mu A\nu''},$$

so that $\mu\mu'$ divides

$$\nu b'b'' + \nu'b''b + \nu''bb' + \Delta\nu\nu'\nu''.$$

It is easy to see that the seven integers $aa'\nu''$, $a'a''\nu$, etc. have no common divisor greater than $\mu\mu'$: hence putting $\mu\mu' = \sigma$, we have

$$\begin{aligned}\sigma = dv\,[&a'a''\nu,\ a''a\nu',\ aa'\nu'',\ a\,(\nu'b'' + \nu''b'),\\ &a'\,(\nu b'' + \nu''b),\ a''\,(\nu b' + \nu'b),\\ &\nu b'b'' + \nu'b''b + \nu''bb' + \Delta\nu\nu'\nu''].\end{aligned}$$

It will be observed that this determination of σ, like that of Δ, is symmetrical with reference to f, f', f''.

Take X, Y to be the variables of F, ξ, η those of Φ: then the successive compositions give rise to the identities

$$\frac{1}{\mu}\,(ax + by + \nu y\sqrt{\Delta})\,(a'x' + b'y' + \nu'y'\sqrt{\Delta})$$
$$= AX + BY + NY\sqrt{\Delta} \ldots\ldots \text{(i)},$$

and

$$\frac{1}{\mu'}\,(AX + BY + NY\sqrt{\Delta})\,(a''x'' + b''y'' + \nu''y''\sqrt{\Delta})$$
$$= \mathbf{A}\xi + \mathbf{B}\eta + \eta\sqrt{\Delta} \ldots\ldots \text{(ii)}.$$

Hence by substitution

$$\mathrm{A}\xi + \mathrm{B}\eta + \eta\sqrt{\Delta}$$
$$= \frac{1}{\sigma}(ax+by+\nu y\sqrt{\Delta})(a'x'+b'y'+\nu'y'\sqrt{\Delta})(a''x''+b''y''+\nu''y''\sqrt{\Delta}) \,.. \text{(iii)}.$$

Now it follows from (ii) that ξ, η are lineo-linear functions of x'', y'', X, Y with *integral* coefficients: and from (i) that X, Y are similar functions of x, y, x', y' with integral coefficients: hence ξ, η are trilinear functions of x, y, x', y', x'', y'' with integral coefficients.

Multiplying out the right-hand side of (iii) and comparing with the left-hand side, we have

$$\eta = \frac{a'a''\nu}{\sigma}x'x''y + \frac{a''a\nu'}{\sigma}x''xy' + \frac{aa'\nu''}{\sigma}xx'y''$$
$$+ \frac{a(\nu'b''+\nu''b')}{\sigma}xy'y'' + \frac{a'(\nu''b+\nu b'')}{\sigma}x'y''y + \frac{a''(\nu b'+\nu'b)}{\sigma}x''yy'$$
$$+ \frac{\nu b'b''+\nu'b''b+\nu''bb'+\Delta\nu\nu'\nu''}{\sigma}yy'y'',$$

and it has in fact been proved that all the seven coefficients are integral and relatively prime.

We have

$$\sigma\mathrm{A}\xi = (ax+by)(a'x'+b'y')(a''x''+b''y'')$$
$$+\Delta\{\nu'\nu''(ax+by)y'y''+\nu''\nu(a'x'+b'y')y''y+\nu\nu'(a''x''+b''y'')yy'\}$$
$$-\sigma\mathrm{B}\eta,$$

and hence we conclude that B simultaneously satisfies the following seven congruences:—

$$\left.\begin{array}{l}
a'a''b - \nu a'a''\,\mathrm{B} \equiv 0 \\
a''ab' - \nu'a''a\,\mathrm{B} \equiv 0 \\
aa'b'' - \nu''aa'\,\mathrm{B} \equiv 0 \\
ab'b'' + \Delta a\nu'\nu'' - a(\nu'b''+\nu''b')\,\mathrm{B} \equiv 0 \\
a'b''b + \Delta a'\nu''\nu - a'(\nu''b+\nu b'')\,\mathrm{B} \equiv 0 \\
a''bb' + \Delta a''\nu\nu' - a''(\nu b'+\nu'b)\,\mathrm{B} \equiv 0 \\
bb'b'' + \Delta(b\nu'\nu''+b'\nu''\nu+b''\nu\nu') \\
\qquad\qquad -(\nu b'b''+\nu'b''b+\nu''bb'+\Delta\nu\nu'\nu'')\,\mathrm{B} \equiv 0
\end{array}\right\} (\text{mod } \sigma\mathrm{A}).$$

Again since B is determinate (mod A), and since in the above congruences all the coefficients of B are divisible by σ, it follows that the seven integers $a'a''b$, $a''ab'$, $aa'b''$, $ab'b''+\Delta a\nu'\nu''$, $a'b''b+\Delta a'\nu''\nu$, $a''bb'+\Delta a''\nu\nu'$, $bb'b''+\Delta\,(b\nu'\nu''+b'\nu''\nu+b''\nu\nu')$ are all divisible by σ, and that the congruences may be replaced by

$$\frac{a'a''b}{\sigma}-\frac{\nu a'a''}{\sigma}\,\mathrm{B}\equiv 0 \pmod{\mathrm{A}},$$

and so on.

Now suppose that by Arndt's process we first compound f' and f'' into F' and then compound F' and f into $(\mathrm{A}', \mathrm{B}', \Gamma')$: and let σ', Δ' be the quantities corresponding to σ, Δ. Then it follows from symmetry that $\sigma'=\sigma$ and $\Delta'=\Delta$: hence $\mathrm{A}'=\mathrm{A}$, and therefore the congruences satisfied by B' are the same as those satisfied by B: hence the forms $(\mathrm{A}', \mathrm{B}', \Gamma')$, $(\mathrm{A}, \mathrm{B}, \Gamma)$ are equivalent, and we may in fact suppose them identical.

This proves that $(KK')\,K''=K\,(K'K'')$, and the symbolical notation for the composition of classes is fully justified, because the commutative and associative laws of multiplication are both satisfied[1]. Instead of $(KK')\,K''$ or $K\,(K'K'')$ we may write without ambiguity $KK'K''$ and call this the class compounded of K, K', K''.

As an example of the direct composition of three forms, let

$$f=(2,\ 1,\ 2)\quad f'=(4,\ 1,\ 7)\quad f''=(3,\ 0,\ 4).$$

Here $\qquad d=-3,\quad d'=-27,\quad d''=-12,$

$\qquad\qquad m=\ \ 2,\quad m'=\ \ 1,\quad m''=\ \ 1:$

and hence $\qquad \Delta=-3,\quad \nu=1,\quad \nu'=3,\quad \nu''=2.$

We find $\qquad \sigma=dv\,(12,\ 18,\ 16,\ 4,\ 8,\ 12,\ -16)$

$\qquad\qquad =2;$

and therefore $\qquad \mathrm{A}=2\,.\,3\,.\,4/2^2=6.$

The congruences to be satisfied by B are

$$\left.\begin{array}{r}6-6\mathrm{B}\equiv 0\\ 3-9\mathrm{B}\equiv 0\\ 8\mathrm{B}\equiv 0\\ 18+2\mathrm{B}\equiv 0\\ 12+4\mathrm{B}\equiv 0\\ 12+6\mathrm{B}\equiv 0\\ 12+8\mathrm{B}\equiv 0\end{array}\right\}\ (\text{mod. } 6),$$

whence $\qquad \mathrm{B}\equiv 3\quad (\text{mod. } 6).$

[1] The distributive law is not required, since such a symbol as $K+K'$ will not occur. Gauss writes $K+K'$ instead of KK': this, of course, is equally legitimate, but not quite so convenient or suggestive.

Taking $\text{B}=3$, we have

$$\Gamma=\frac{\text{B}^2-\Delta}{\text{A}}=2:$$

so that the result of the composition is

$$(6,\ 3,\ 2)\sim(2,\ 1,\ 2).$$

This, of course, might have been foreseen, on finding $\Delta=-3$; for it is clear that the resultant class will be improperly primitive, and there is only one such class for $\Delta=-3$.

If we wish to find the trilinear substitution which transforms (A, B, Γ) or (6, 3, 2) into $ff'f''$, we put

$$\tfrac{1}{2}(2x+y+y\surd-3)(4x'+y'+3y'\surd-3)(3x''+2y''\surd-3)$$
$$=6x+3y+y\surd-3,$$

and hence by expanding, and comparing both sides,

$$Y=\qquad 6x'x''y+9x''xx'+8xx'y''+2xy'y''+4x'y''y+6x''yy'-8yy'y'',$$
$$X=2xx'x''-2x'x''y-4x''xy'-4xx'y''-4xy'y''-4x'y''y-5x''yy'+2yy'y''.$$

144. It is now evident that if $f_1, f_2\ldots f_n$ are any number of forms whose determinants are proportional to n square numbers, and if $K_1, K_2\ldots K_n$ are the classes to which they belong, then it is possible to find a form compounded of $f_1, f_2\ldots f_n$; and in whatever order the forms are compounded, the resulting form will belong to one and the same class, whose determinant

$$\Delta=dv\,(d_1m_2{}^2m_3{}^2\ldots m_n{}^2,\ d_2m_1{}^2m_3{}^2\ldots m_n{}^2,\ d_nm_1{}^2m_2{}^2\ldots m_{n-1}{}^2),$$

taken with the same sign as that of $d_1, d_2\ldots d_n$. This class may therefore be denoted without ambiguity by $K_1K_2\ldots K_n$. The classes K need not be all different: thus we may have such compositions as are denoted by $K_1{}^3$, $K_1{}^2K_2{}^2$, and so on.

145. Consider more particularly the composition of two forms f, f' of the same determinant and for which m, m' are relatively prime. Then if D be the determinant of the form $F=(A,\ B,\ C)$ compounded of them, we have

$$D=d=d',\ n=n'=1, \quad \text{and} \quad \mu=dv\,(a,\ a',\ b+b').$$

Putting, as before, $A=aa'/\mu^2$, B is determined by the congruences

$$\left.\begin{aligned}\frac{a}{\mu}B&\equiv\frac{ab'}{\mu}\\ \frac{a'}{\mu}B&\equiv\frac{a'b}{\mu}\\ \frac{b+b'}{\mu}B&\equiv\frac{bb'+D}{\mu}\end{aligned}\right\}(\text{mod A}).$$

Also $$M = dv\,(A, 2B, C) = mm' :$$
and if $\mathfrak{M} = dv\,(A, B, C)$, $\mathfrak{m} = dv\,(a, b, c)$, $\mathfrak{m}' = dv\,(a', b', c')$, then if $\mathfrak{m} = m$ *and* $\mathfrak{m}' = m'$, $\mathfrak{M} = M$, while in every other case $\mathfrak{M} = \frac{1}{2}M$.

Hence we at once infer the following conclusions:—

(i) If f' is properly primitive, F belongs to the same order as f.

(ii) Any class is unaltered by composition with the principal class.

For if $f' = (1, 0, -D)$, we have $\mu = 1$, $A = a$, and the congruences to find B are
$$aB \equiv 0, \quad B \equiv b, \quad bB \equiv D \pmod{a},$$
whence $B \equiv b \pmod{a}$, and $F \backsim f$.

If then H denote the principal class, so far as composition is concerned we may write $H = 1$.

(iii) Two opposite properly primitive classes compound into the principal class.

Namely if $f = (a, b, c)$, $f' = (a, -b, c)$,
$$\mu = a, \quad A = 1, \quad B \equiv 0 \pmod{\mathrm{A}},$$
and $$F = (1, 0, -D).$$

Hence if K denote a properly primitive class, we may express its opposite by K^{-1}.

(iv) If K is a properly primitive class, and Φ any class, there is one and only one class which compounded with K will give Φ: namely ΦK^{-1}.

(v) If K is properly primitive, and $\Phi_1, \Phi_2 \ldots \Phi_n$ are all different, then $K\Phi_1, K\Phi_2 \ldots K\Phi_n$ are all different.

For if we suppose $K\Phi_1 = K\Phi_2$, then compounding each with K^{-1}, we get $\Phi_1 = \Phi_2$ contrary to hypothesis.

(vi) The duplication of a properly primitive *ambiguous* class produces the principal class.

For an ambiguous class is its own opposite: so that, if K is a properly primitive ambiguous class, $K = K^{-1}$, and therefore $K^2 = KK^{-1} = 1$.

Conversely, if $K^2 = 1$, $K^{-1} = K^2K^{-1} = K\,(KK^{-1}) = K$; that is, K is its own opposite, and therefore ambiguous.

(vii) The class compounded of the opposites of any number of properly primitive classes is the opposite of the class compounded of those classes.

For example, $(K^{-1}L^{-1})(KL) = K^{-1}K \,.\, L^{-1}L = 1$: therefore $K^{-1}L^{-1} = (KL)^{-1}$: and so for any number of classes.

In particular, the class compounded of any number of ambiguous classes is itself ambiguous.

146. We are now able to compare the numbers of classes belonging to the different orders of a given determinant D.

Suppose D is divisible by a square number m^2, and let $D = \Delta m^2$. Then there will be an order Ω derived from the properly primitive order of determinant Δ. As the simplest representative form of this order we may take $(m, 0, -m\Delta)$. If $\Delta \equiv 1 \pmod 4$ there will also be an order Ω' derived from an improperly primitive order of determinant Δ: and we may take for its simplest representative form $(2m, m, \frac{1}{2}m(1-\Delta))$.

Now let $f = (a, b, c)$ be any properly primitive form of determinant Δ: and let us suppose, as we may do (see Art. 127) that a is prime to $2m\Delta$: then the form (a, bm, cm^2) is properly primitive, and it is easily verified that (ma, mb, mc) is compounded of (a, bm, cm^2) and $(m, 0, -m\Delta)$.

Similarly every class of the order Ω' will contain a form $(2ma, mb, 2mc)$ in which a is prime to $2m\Delta$: and this form is compounded of $(2m, m, \frac{1}{2}m(1-\Delta))$ and $(a, mb, 4m^2c)$, the latter of which is properly primitive.

We conclude therefore that every class of a derived order may be obtained by compounding the simplest class of that order with a properly primitive class.

Again, every class of the order may be obtained by compounding any *assigned* class of the order with a properly primitive class. For let Φ be the assigned class, Φ' any other class, Φ_0 the simplest class, K, L properly primitive classes which compounded with Φ_0 give Φ, Φ' respectively. Then $\Phi = \Phi_0 K$, $\Phi' = \Phi_0 L = \Phi L K^{-1}$: that is, Φ' is obtained from Φ by compounding it with the properly primitive class LK^{-1}.

Now let $\Phi_1, \Phi_2 \ldots \Phi_\nu$ be all the classes belonging to a given derived order: and let $F_1, F_2 \ldots F_n$ be all the properly primitive classes of the same determinant. Then the classes $F_1\Phi_1, F_2\Phi_1 \ldots F_n\Phi_1$

include *all* the classes Φ; therefore ν cannot exceed n. It can easily be shown that n is a multiple of ν. In fact, if $n > \nu$, some two or more of the classes $F_1\Phi_1, F_2\Phi_1 \ldots F_n\Phi_1$ must be identical. Suppose

$$F_1\Phi_1 = F_2\Phi_1 = \ldots = F_k\Phi_1.$$

Let F_1' be any properly primitive class not contained in $F_1, F_2 \ldots F_k$, and let $K = F_1'F_1^{-1}$, so that $F_1' = KF_1$: then $KF_1, KF_2 \ldots KF_k$ will be properly primitive classes different from each other and from the preceding set; and putting $KF_i = F_i'$, we have

$$F_1'\Phi_1 = F_2'\Phi_1 = \ldots = F_k'\Phi_1.$$

Proceeding in this way, we see (as in a similar case, Art. 18) that $F_1\Phi_1, F_2\Phi_1 \ldots F_n\Phi_1$ may be arranged in groups each containing k identical classes, the classes of any two groups being different; and therefore $n = \nu k$, that is, n is a multiple of ν.

147. It is evident that k is equal to the number of properly primitive classes which, compounded with the simplest (or any other) class of the derived order, reproduce that class: and the problem of determining k was considered from this point of view by Gauss[1], who did not, however, succeed in obtaining a complete solution. The following investigation, which depends on the theory of transformation, is due to Lipschitz[2].

We consider in the first place two determinants D and $D' = Dp^2$, where p is a prime.

Let $f = (a, b, c)$ be any properly primitive form of determinant D, and let us suppose that a is prime to p. Then applying to f the substitution

$$P = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix},$$

where
$$\alpha\delta - \beta\gamma = p,$$

or, say, a substitution of order p, we obtain

$$f' = Pf = (a', b', c'), \text{ suppose,}$$

a form of determinant Dp^2. Suppose that all possible substitutions P are applied to f, and let us examine how the resulting forms may be classified.

[1] D. A. Arts. 253—6.

[2] Crelle liii. (1857), p. 238.

Let $U = \begin{pmatrix} \alpha', & \beta' \\ \gamma', & \delta' \end{pmatrix}$, where $\alpha'\delta' - \beta'\gamma' = 1$, be any unitary substitution: then

$$PU = \begin{pmatrix} \alpha, & \beta \\ \gamma, & \delta \end{pmatrix} \begin{pmatrix} \alpha', & \beta' \\ \gamma', & \delta' \end{pmatrix} = \begin{pmatrix} \alpha\alpha' + \beta\gamma', & \alpha\beta' + \beta\delta' \\ \gamma\alpha' + \delta\gamma', & \gamma\beta' + \delta\delta' \end{pmatrix} = P', \text{ say,}$$

is a substitution of order p. It is clear that the forms Pf and $P'f$ are equivalent, the first being transformed into the second by the substitution U. The substitutions P, P' may be called equivalent: and we need only consider the non-equivalent P-substitutions.

Since $\alpha\delta - \beta\gamma = p$, and p is prime, it is evident that $dv(\gamma, \delta) = 1$ or p.

First, let $dv(\gamma, \delta) = 1$: then putting $\alpha' = \delta$, $\gamma' = -\gamma$, and determining β', δ' so that $\alpha'\delta' - \beta'\gamma' = \gamma\beta' + \delta\delta' = 1$, the substitution PU or P' becomes $\begin{pmatrix} p, & h \\ 0, & 1 \end{pmatrix}$. Moreover the general values of β', δ' are of the form $\beta_0' + k\delta$, $\delta_0' - k\gamma$, where k is any integer: hence $h = \alpha\beta_0' + \beta\delta_0' + k(\alpha\delta - \beta\gamma) = h_0 + kp$: we may therefore suppose that h is replaced by its least positive residue (mod p).

Similarly, if $dv(\gamma, \delta) = p$, we may put $\alpha' = \delta/p$, $\gamma' = -\gamma/p$, and then determine β', δ' so that $\alpha'\delta' - \beta'\gamma' = 1$, and $PU = \begin{pmatrix} 1, & 0 \\ 0, & p \end{pmatrix}$.

Hence every substitution of order p is equivalent to one of the following $(p+1)$ representative substitutions:

$$\begin{pmatrix} 1, & 0 \\ 0, & p \end{pmatrix},$$

$$\begin{pmatrix} p, & h \\ 0, & 1 \end{pmatrix} \quad (h = 0, 1, 2 \ldots \overline{p-1}).$$

148. We will now apply these $(p+1)$ substitutions to the properly primitive form (a, b, c) of determinant D.

First let p be an *odd* prime.

Then $\begin{pmatrix} 1, & 0 \\ 0, & p \end{pmatrix} (a, b, c) = (a, bp, cp^2)$, and this is properly primitive, since a is prime to p.

Again $$\begin{pmatrix} p, & h \\ 0, & 1 \end{pmatrix} (a, b, c) = (a', b', c'),$$

where
$$a' = ap^2,$$
$$b' = (ah + b)p,$$
$$c' = ah^2 + 2bh + c.$$

From these equations we deduce

$$p^2 a = a',$$
$$p^2 b = pb' - ha',$$
$$p^2 c = p^2 c' - 2phb' - h^2 a',$$

and since $dv\,(a,\ 2b,\ c) = 1$, we infer that

$$dv\,(a',\ 2b',\ c') = 1,\ p \text{ or } p^2.$$

Now $ac' = (ah + b)^2 - D$: and therefore if p divides c' it will be possible to choose h so that

$$(ah + b)^2 - D \equiv 0 \pmod{p},$$

and since a is prime to p the converse is true.

There are four cases to consider:—

(i) D divisible by p^2. The congruence in h has one solution, given by $ah + b \equiv 0 \pmod{p}$: this value of h makes b' and c' divisible by p^2: so that in all there are p properly primitive forms $(a',\ b',\ c')$ and one form for which $dv\,(a',\ 2b',\ c') = p^2$.

(ii) D divisible by p but not by p^2. As before, the congruence has one root, and for the corresponding form, f', $dv\,(a',\ 2b',\ c') = p$. The remaining p forms f' are properly primitive.

(iii) D not divisible by p, and $(D \mid p) = 1$. The congruence has two roots given by

$$ah + b \pm \sqrt{D} \equiv 0 \pmod{p}:$$

there are two forms f' for which $dv\,(a',\ 2b',\ c') = p$, and $(p - 1)$ properly primitive forms.

(iv) D not divisible by p, and $(D \mid p) = -1$. The congruence is insoluble, and all the $(p + 1)$ forms f' are properly primitive.

In every case the number of properly primitive forms f' may be expressed by $p - (D|p)$, with the convention that $(D \mid p) = 0$ when $D \equiv 0 \pmod{p}$.

Next, let $p = 2$.

Here $\begin{pmatrix}1, & 0\\ 0, & 2\end{pmatrix}(a,\ b,\ c) = (a,\ 2b,\ 4c)$, which is properly primitive, since a is supposed odd.

Again $\begin{pmatrix}2, & h\\ 0, & 1\end{pmatrix}(a,\ b,\ c)$ is properly primitive except when

$$(ah + b)^2 - D \equiv 0 \pmod{2}.$$

If D is odd the congruence has one root given by

$$ah + b \equiv 1 \pmod 2,$$

and if D is even, there is again one solution given by

$$ah + b \equiv 0 \pmod 2.$$

In the former case, $dv\,(a', b', c') = 2$, and $dv\,(a', 2b', c') = 2$ or 4 according as $D \equiv 3$ or $1 \pmod 4$: in the latter,

$$dv\,(a', b', c') = dv\,(a', 2b', c') = 2 \text{ or } 4$$

according as $D \equiv 2$ or $0 \pmod 4$.

In every case there are two properly primitive forms.

149. Every properly primitive class of determinant Dp^2 can be derived from a properly primitive class of determinant D by means of one of the $(p+1)$ representative substitutions of order p.

For let (A, B, C) be any properly primitive form of determinant Dp^2, in which A is prime to p. Apply to it all possible substitutions of order p: then the resulting forms of determinant Dp^4 fall into $(p+1)$ sets, the forms of each set being equivalent, and those of one set, and only one, having a divisor p^2. Suppose

$$\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}(A, B, C) = (p^2a, p^2b, p^2c),$$

where $\alpha\delta - \beta\gamma = p$; then (a, b, c) is a properly primitive form of determinant D: and it is easily verified that

$$\begin{pmatrix}\delta, & -\beta\\ -\gamma, & \alpha\end{pmatrix}(a, b, c) = (A, B, C);$$

that is, (A, B, C) is derivable from (a, b, c) by the substitution $\begin{pmatrix}\delta, & -\beta\\ -\gamma, & \alpha\end{pmatrix}$. Moreover the class to which (a, b, c) belongs is perfectly determinate. For if

$$\begin{pmatrix}\delta', & -\beta'\\ -\gamma', & \alpha'\end{pmatrix}(a', b', c') = \begin{pmatrix}\delta, & -\beta\\ -\gamma, & \alpha\end{pmatrix}(a, b, c)$$
$$= (A, B, C),$$

then

$$\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}(A, B, C) = (p^2a, p^2b, p^2c),$$

and

$$\begin{pmatrix}\alpha', & \beta'\\ \gamma', & \delta'\end{pmatrix}(A, B, C) = (p^2a', p^2b', p^2c'):$$

but all the forms of divisor p^2 derivable from (A, B, C) belong to the same class: therefore $(p^2a', p^2b', p^2c') \sim (p^2a, p^2b, p^2c)$ and consequently $(a', b', c') \sim (a, b, c)$.

150. If now $f_1, f_2 \ldots f_n$ are representatives of the n properly primitive classes of determinant D, the first coefficient of each form being prime to p, and if we apply to each of them the $(p+1)$ reduced substitutions of order p, we obtain altogether $n\{p-(D|p)\}$ properly primitive forms of determinant Dp^2, among which will be found representatives of *all* the properly primitive classes. It remains for us to discover how many of these are equivalent. It follows from the last paragraph, and from the fact that $f_1, f_2 \ldots f_n$ all belong to different classes, that any two such equivalent forms must be derived from the *same* form f. Suppose then that

$$\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}(a,\ b,\ c) = (A,\ B,\ C),$$

$$\begin{pmatrix}\alpha', & \beta'\\ \gamma', & \delta'\end{pmatrix}(a,\ b,\ c) = (A',\ B',\ C'),$$

where $\alpha\delta - \beta\gamma = \alpha'\delta' - \beta'\gamma' = p$, and $(A',\ B',\ C') \backsim (A,\ B,\ C)$.

If the unitary substitution $\begin{pmatrix}\lambda, & \mu\\ \nu, & \rho\end{pmatrix}$ transforms $(A',\ B',\ C')$ into $(A,\ B,\ C)$, then

$$\begin{pmatrix}\alpha', & \beta'\\ \gamma', & \delta'\end{pmatrix}\begin{pmatrix}\lambda, & \mu\\ \nu, & \rho\end{pmatrix}$$

changes $(a,\ b,\ c)$ into $(A,\ B,\ C)$ and must therefore be of the form

$$\begin{pmatrix}T_i - bU_i, & -cU_i\\ aU_i, & T + bU_i\end{pmatrix}\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix},$$

where $(T_i,\ U_i)$ is an integral solution of $T^2 - DU^2 = 1$. Operating on both substitutions with $\begin{pmatrix}\delta', & -\beta'\\ -\gamma', & \alpha'\end{pmatrix}$, we get

$$\begin{pmatrix}p\lambda, & p\mu\\ p\nu, & p\rho\end{pmatrix} = \begin{pmatrix}\delta', & -\beta'\\ -\gamma', & \alpha'\end{pmatrix}\begin{pmatrix}T_i - bU_i, & -cU_i\\ aU_i, & T_i + bU_i\end{pmatrix}\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$$

$$= \begin{pmatrix}\mathbf{A}, & \mathbf{B}\\ \mathbf{\Gamma}, & \mathbf{\Delta}\end{pmatrix} \text{ say:}$$

so that the conditions for equivalence are expressed by

$$\mathbf{A} \equiv \mathbf{B} \equiv \mathbf{\Gamma} \equiv \mathbf{\Delta} \equiv 0 \pmod{p}.$$

Since $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}$ and $\begin{pmatrix}\alpha', & \beta'\\ \gamma', & \delta'\end{pmatrix}$ may be taken from the reduced substitutions of order p, there are only two distinct cases to consider.

First, let $\begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix} = \begin{pmatrix}p, & h\\ 0, & 1\end{pmatrix}$, $\begin{pmatrix}\alpha', & \beta'\\ \gamma', & \delta'\end{pmatrix} = \begin{pmatrix}1, & 0\\ 0, & p\end{pmatrix}$; then it will be found by actual calculation that

$$\begin{aligned}
\mathrm{A} &= p^2(T_i - bU_i),\\
\mathrm{B} &= p\,\{h(T_i - bU_i) - cU_i\},\\
\Gamma &= paU_i,\\
\Delta &= T_i + (ah + b)U_i.
\end{aligned}$$

The single condition necessary for equivalence is therefore

$$T_i + (ah + b)U_i \equiv 0 \pmod{p}.$$

Since a is prime to p, this gives one determinate value for h, such that $0 \leqq h < p$, *except when* $U_i \equiv 0$ (*mod* p). Let U_σ be the least positive value of U_i which is divisible by p; then putting $i = 1, 2 \ldots (\sigma - 1)$ in the above congruence we get $(\sigma - 1)$ corresponding values of h. Call these $h_1, h_2 \ldots h_{\sigma-1}$, each being positive and less than p. Then the forms

$$\begin{pmatrix}p, & h_i\\ 0, & 1\end{pmatrix}(a, b, c) \qquad (i = 1, 2 \ldots \sigma - 1)$$

are all equivalent to $\begin{pmatrix}1, & 0\\ 0, & p\end{pmatrix}(a, b, c)$. Moreover they are all different, and there are no other forms

$$\begin{pmatrix}p, & h\\ 0, & 1\end{pmatrix}(a, b, c) \text{ equivalent to } \begin{pmatrix}1, & 0\\ 0, & p\end{pmatrix}(a, b, c).$$

For, supposing neither U_i nor $U_j \equiv 0 \pmod{p}$ we have

$$\begin{aligned}
h_j - h_i &\equiv \frac{T_i + bU_i}{aU_i} - \frac{T_j + bU_j}{aU_j} \pmod{p}\\
&\equiv \frac{T_iU_j - T_jU_i}{aU_iU_j}\\
&\equiv \frac{U_{j-i}}{aU_iU_j}
\end{aligned}$$

and therefore $h_j = h_i$, if and only if $U_{j-i} \equiv 0 \pmod{p}$ that is, if $j - i \equiv 0 \pmod{\sigma}$.

Altogether then we have a set of σ equivalent forms derived from (a, b, c) by the substitutions

$$\begin{pmatrix}1, & 0\\ 0, & p\end{pmatrix} \quad \begin{pmatrix}p, & h_i\\ 0, & 1\end{pmatrix} \qquad (i = 1, 2 \ldots \sigma - 1).$$

In a similar way we find that

$$\begin{pmatrix} p, & h' \\ 0, & 1 \end{pmatrix}(a, b, c) \sim \begin{pmatrix} p, & h \\ 0, & 1 \end{pmatrix}(a, b, c),$$

if $$(h-h')\,T_i - \{hh'a + (h+h')\,b + c\}\,U_i = 0 \pmod{p},$$

that is, if $$h' \equiv \frac{h\,(T_i - bU_i) - cU_i}{haU_i + (T_i + bU_i)} \pmod{p}.$$

Let h_i' be the least positive value of h' derived from this congruence. It is clear that the value of h_i' is determinate except when there is a solution of the Pellian equation such that

$$haU_i + (T_i + bU_i) \equiv 0 \pmod{p},$$

in which case $\begin{pmatrix} p, & h \\ 0, & 1 \end{pmatrix}(a, b, c) \sim \begin{pmatrix} 1, & 0 \\ 0, & p \end{pmatrix}(a, b, c)$ by the preceding case.

We also find that

$$h_j' - h_i' \equiv \frac{(ah^2 + 2bh + c)\,U_{j-i}}{\{haU_i + (T_i + bU_i)\}\,\{haU_j + (T_j + bU_j)\}} \pmod{p}.$$

If $ah^2 + 2bh + c \equiv 0 \pmod{p}$, $\begin{pmatrix} p, & h \\ 0, & 1 \end{pmatrix}(a, b, c)$ is not properly primitive; rejecting these cases, when they exist, we see that $h_j' = h_i'$ if and only if $j \equiv i \pmod{\sigma}$.

As before, we have a set of σ equivalent forms, viz. these are derived from (a, b, c) by the substitutions

$$\begin{pmatrix} p, & h_1' \\ 0, & 1 \end{pmatrix}, \begin{pmatrix} p, & h_2' \\ 0, & 1 \end{pmatrix} \cdots \begin{pmatrix} p, & h_\sigma' \\ 0, & 1 \end{pmatrix},$$

(where observe $h_\sigma' = h$), or else by the substitutions

$$\begin{pmatrix} p, & h_1' \\ 0, & 1 \end{pmatrix}, \begin{pmatrix} p, & h_2' \\ 0, & 1 \end{pmatrix} \cdots \begin{pmatrix} p, & h_{i-1}' \\ 0, & 1 \end{pmatrix}, \begin{pmatrix} 1, & 0 \\ 0, & p \end{pmatrix}, \begin{pmatrix} p, & h_{i+1}' \\ 0, & 1 \end{pmatrix} \cdots \begin{pmatrix} p, & h_\sigma' \\ 0, & 1 \end{pmatrix}$$

according as h does not, or does, satisfy a congruence of the form

$$haU_i + (T_i + bU_i) \equiv 0 \pmod{p}.$$

Since the same reasoning applies whichever form (a, b, c) be taken, we conclude that the total number of properly primitive classes of determinant Dp^2 is

$$\frac{n}{\sigma}\,\{p - (D|p)\} = \frac{np}{\sigma}\left\{1 - \frac{1}{p}\,(D|p)\right\};$$

σ having the meaning above explained, and $(D|p)$ being put equal to 0 if D is divisible by p, or if $p = 2$.

151. By successive applications of this result it is easy to conclude that if $D' = DS^2$, and n, n' are the numbers of properly primitive classes of determinants D, D' respectively,

$$n' = \frac{nS}{\sigma} \cdot \Pi \left\{1 - \frac{1}{p}(D|p)\right\},$$

where the product relates to all odd primes p which divide S, but not D, and where σ is the index of the first integral solution (T_σ, U_σ) of $T^2 - DU^2 = 1$ for which U_σ is divisible by S. The result may also be expressed in the form

$$n' = nS \cdot \frac{\log(T + U\sqrt{D})}{\log(T' + U'\sqrt{D'})} \Pi \left\{1 - \frac{1}{p}(D|p)\right\},$$

where (T, U), (T', U') are the fundamental solutions of $T^2 - DU^2 = 1$, and $T'^2 - D'U'^2 = 1$ respectively. In this form it was originally obtained by Dirichlet, although by means of a very different method, which will be explained later on.

When D', and therefore D, is negative, the Pellian equation has in general only two solutions, viz. $T = \pm 1$, $U = 0$: it is easily seen from the foregoing analysis that all the substitutions of order p give non-equivalent forms, and that

$$n' = nS\Pi \left\{1 - \frac{1}{p}(D|p)\right\}.$$

If, however, $D = -1$, the equation $T^2 - DU^2 = 1$ has four solutions, $T = \pm 1$, $U = 0$, and $T = 0$, $U = \pm 1$; the derived forms may be grouped into equivalent pairs, and

$$n' = \tfrac{1}{2}nS \cdot \Pi \left\{1 - \frac{(-1)^{\frac{1}{2}(p-1)}}{p}\right\}.$$

152. It will be observed that the preceding analysis enables us not only to determine the number of properly primitive classes for a determinant DS^2 when that for a determinant D is known, but also to compare the numbers of properly primitive classes for any two determinants which are in the ratio of two square numbers. It is clear also that we can find the ratios of the numbers of classes in the different derived orders for any determinant, because the number of classes in any derived order is equal to the number of (properly or improperly) primitive classes for the determinant from which the order is derived.

153. In order to complete the investigation, we have to compare the number of improperly primitive classes with that of the properly primitive classes for the same determinant.

Let $\phi = (2a,\ b,\ 2c)$ be an improperly primitive form of determinant

$$D = b^2 - 4ac \equiv 1 \pmod{4}:$$

and suppose (as we may do) that a is odd. Applying to ϕ the reduced substitutions of order 2, viz.

$$\begin{pmatrix}1, & 0\\ 0, & 2\end{pmatrix},\quad \begin{pmatrix}2, & 0\\ 0, & 1\end{pmatrix},\quad \begin{pmatrix}2, & 1\\ 0, & 1\end{pmatrix},$$

we obtain $2\phi_1$, $2\phi_2$, $2\phi_3$ where

$$\phi_1 = (a,\ b,\ 4c),$$
$$\phi_2 = (4a,\ b,\ c),$$
$$\phi_3 = (4a,\ 2a + b,\ a + b + c).$$

The first of these is properly primitive: with regard to the others we have to distinguish the cases $D \equiv 1 \pmod{8}$ and $D \equiv 5 \pmod{8}$.

If $D \equiv 1 \pmod{8}$, a, b are odd, c is even, and therefore ϕ_2, ϕ_3 are improperly primitive. Thus ϕ is transformable into the double of one and only one properly primitive form: and it may be proved as above (Art. 149) that the double of every properly primitive form is derivable from an improperly primitive form by a substitution of order 2. Hence if $D \equiv 1 \pmod{8}$ the numbers of properly and improperly primitive classes are equal.

If $D \equiv 5 \pmod{8}$, c is odd, and ϕ_1, ϕ_2, ϕ_3 are all properly primitive: we have to discover how many of them are equivalent.

Suppose that

$$(4a,\ b,\ c) = \begin{pmatrix}\alpha, & \beta\\ \gamma, & \delta\end{pmatrix}(a,\ b,\ 4c),\quad (\alpha\delta - \beta\gamma = 1),$$

then

$$4a = a\alpha^2 + 2b\alpha\gamma + 4c\gamma^2 \dots\dots\dots\dots(1),$$
$$b = a\alpha\beta + b(\alpha\delta + \beta\gamma) + 4c\gamma\delta \dots\dots\dots\dots(2),$$
$$c = a\beta^2 + 2b\beta\delta + 4c\delta^2 \quad \dots\dots\dots\dots(3),$$
$$\therefore\quad 0 = a\alpha\beta + 2b\beta\gamma + 4c\gamma\delta \dots\dots\dots\dots(4),$$

and hence

$$c\gamma = a\beta(\beta\gamma - \alpha\delta) = -a\beta.$$

Putting

$$\gamma = aU,\quad \beta = -cU,$$

(4) gives

$$\alpha - 4\delta = -2bU,$$

and writing $$\alpha + 4\delta = 2T,$$
where T is evidently integral, we have
$$\alpha = T - bU,$$
$$\delta = (T + bU)/4.$$

Now from (1) we obtain
$$4a^2 = (a\alpha + b\gamma)^2 - D\gamma^2,$$
and on substituting for α, γ their values, a^2 divides out, and we find
$$T^2 - DU^2 = 4.$$

The condition for equivalence is therefore that solutions of $T^2 - DU^2 = 4$ must exist for which
$$T + bU \equiv 0 \pmod{4}.$$

We have $$(T + bU)(T - bU) = 4(1 - acU^2),$$
and a, c are both odd. If, then, U is even, $T + bU$ cannot be divisible by 4: for if it were, $T - bU$ would be odd, and
$$(T - bU) + (T + bU) = 2T$$
would be odd, which is absurd, since T is supposed integral. Therefore U *must be odd.* Conversely if U is odd, T and bU are both odd, and therefore by taking U with the proper sign we can make $T + bU$ divisible by 4.

If (T_1, U_1) is the fundamental solution, and U_1 is even, all the subsequent values of U will be even too; therefore U_1 must be odd.

Suppose this to be the case, and let the sign of U_1 be chosen so that
$$T_1 + bU_1 \equiv 0 \pmod{4}.$$

Then putting
$$\alpha_1 = T_1 - bU_1, \quad \beta_1 = -cU_1,$$
$$\gamma_1 = aU_1, \qquad \delta_1 = \tfrac{1}{4}(T_1 + bU_1),$$
$\begin{pmatrix}\alpha_1, & \beta_1 \\ \gamma_1, & \delta_1\end{pmatrix}$ is an integral unitary substitution which transforms $(a, b, 4c)$ into $(4a, b, c)$.

Changing the sign of U_1, put
$$\alpha_2 = T_1 + bU_1, \quad \beta_2 = cU_1,$$
$$\gamma_2 = -aU_1, \qquad \delta_2 = \tfrac{1}{4}(T_1 - bU_1),$$
then δ_2 is half an odd integer: α_2 is divisible by 4, β_2, γ_2 are odd.

Hence $$\tfrac{1}{2}(\alpha_2 + 2\beta_2), \quad \tfrac{1}{2}(\gamma_2 + 2\delta_2)$$
are integers, and it may be verified that

$$\begin{pmatrix} \alpha_2, & \frac{1}{2}(\alpha_2 + 2\beta_2) \\ \gamma_2, & \frac{1}{2}(\gamma_2 + 2\delta_2) \end{pmatrix}$$

is an integral unitary substitution, which transforms $(a, b, 4c)$ into

$$(4a, \; 2a + b, \; a + b + c).$$

Expressed in terms of $\alpha_1, \beta_1, \gamma_1, \delta_1$ this substitution is

$$\begin{pmatrix} 4\delta_1, & 2\delta_1 - \beta_1 \\ -\gamma_1, & \frac{1}{4}(\alpha_1 - 2\gamma_1) \end{pmatrix}.$$

We conclude, then, that if U_1 is even, no two of the forms ϕ_1, ϕ_2, ϕ_3 are equivalent, and that if U_1 is odd, they all belong to the same class.

When D is negative, the equation $T^2 - DU^2 = 4$ has in general only two solutions $T = \pm 2$, $U = 0$; the only exception is when $D = -3$, in which case there are six solutions $T = \pm 1$, $U = \pm 1$, $T = \pm 2$, $U = 0$. Thus when $D = -3$, ϕ_1, ϕ_2, ϕ_3 are all equivalent: for all other negative determinants they belong to three different classes.

The results thus obtained are exhibited in the following table, where n, n' denote the number of properly and improperly primitive classes respectively, and (T_1, U_1) is the fundamental solution of $T^2 - DU^2 = 4$.

I. D positive.

$D \equiv 1 \pmod 8$, $\quad n' = n$,

$D \equiv 5 \pmod 8$, U_1 odd: $\quad n' = n$,

$D \equiv 5 \pmod 8$, U_1 even: $\quad n' = \frac{1}{3} n$.

II. D negative.

$D \neq -3$, $\quad n' = \frac{1}{3} n$,

$D = -3$, $\quad n' = n$.

As an illustration suppose $D = 21$, $\phi = (6, 3, -2)$. The associated forms are

$$\phi_1 = (3, 3, -4), \quad \phi_2 = (12, 3, -1), \quad \phi_3 = (12, 9, 5).$$

We have $T_1 = 5$, $U_1 = 1$, and calculating $\alpha_1, \beta_1, \gamma_1, \delta_1$ it will be found that

$$\begin{pmatrix} 2, & 1 \\ 3, & 2 \end{pmatrix}(3, 3, -4) = (12, 3, -1),$$

$$\begin{pmatrix} 8, & 3 \\ -3, & -1 \end{pmatrix}(3, 3, -4) = (12, 9, 5),$$

and hence $n' = n$, as it should be.

It may be inferred from the foregoing, and can be proved independently, that when U_1 is odd, U_2 is also odd, and U_3 even: in fact, the solutions (T_i, U_i) fall into three sets corresponding to the triple grouping of the properly primitive with reference to the improperly primitive classes.

Composition of Genera.

154. Let K, K' be two properly primitive classes of determinant D, and let n, n' be two numbers prime to each other and to $2D$ representable by forms of the classes K, K' respectively; then it follows from the theory of the composition of classes that nn' is representable by a form of the class KK' which is compounded of K and K'. The generic character of KK' may therefore be inferred from nn'; and it is easily seen that any particular character relating to KK' may be obtained by multiplying together the corresponding characters relating to K and K'.

For the quadratic characters this is obvious since

$$(nn' | p) = (n | p)(n' | p).$$

With regard to the supplementary characters χ, ψ, we have

$$(n-1)(n'-1) \equiv 0 \pmod 4,$$

so that
$$(n-1) + (n'-1) \equiv (nn'-1) \pmod 4,$$

therefore
$$\tfrac{1}{2}(n-1) + \tfrac{1}{2}(n'-1) \equiv \tfrac{1}{2}(nn'-1) \pmod 2,$$

and hence
$$\chi(K)\chi(K') = \chi(KK'):$$

again
$$(n^2-1)(n'^2-1) \equiv 0 \pmod{64},$$

whence
$$\tfrac{1}{8}(n^2n'^2-1) = \tfrac{1}{8}(n^2-1) + \tfrac{1}{8}(n'^2-1) \pmod 8,$$

and therefore
$$\psi(KK') = \psi(K)\psi(K').$$

The genus to which KK' belongs is said to be compounded of the genera which contain K, K'; and the genus compounded of the genera Γ, Δ may be represented by $\Gamma\Delta$. The composition of any genus with itself gives the principal genus, i.e. that which contains the principal class.

If one of the classes K, K' is improperly and the other properly primitive, KK' is improperly primitive; and it is easily seen that, as before, its particular characters are obtained by multiplying together those of K and K'.

If both K and K' are improperly primitive, KK' is the double of a properly primitive class, and the characters of this properly primitive class are obtained by multiplying together those of K and K'. For if $2n$, $2n'$ are two numbers representable by K and K' respectively, n, n' being prime to each other and to $2D$, the particular characters of K, K' are inferred from n and n': and if $KK' = 2L$, the characters of L are inferred from nn', since $2nn'$ is representable by KK', and therefore nn' by L.

155. *Each genus of the same order contains the same number of classes.*

Let Γ, Γ' be any two genera of the same order, and let Γ contain the classes K_1, $K_2 \ldots K_\nu$. Suppose K' to be any class contained in Γ', and let P be a properly primitive class such that $PK_1 = K'$. Then the classes PK_1, $PK_2 \ldots PK_\nu$ will all be different and will all belong to Γ', since their total characters are the same. Hence Γ' contains at least as many classes as Γ. In the same way Γ contains at least as many as Γ'. Therefore they contain the same number of classes.

Number of Ambiguous Classes.

156. The following is Gauss's investigation of the number of properly primitive ambiguous classes for a given determinant D. In order to avoid a trivial exception, it will be supposed that D is not equal to -1. This case is immediately disposed of by observing that, when $D = -1$, there is only one class and this is ambiguous.

It will be remembered that a form (a, b, c) is ambiguous if $2b \equiv 0 \pmod{a}$; also that $(a, b', c') \sim (a, b, c)$ if $b' \equiv b \pmod{a}$, the determinant being the same in both cases. It is therefore only necessary to consider forms of the types $(a, 0, c)$ and $(2b, b, c)$.

We obtain a properly primitive form $(a, 0, c)$ by resolving D into any two factors which are prime to each other, and taking one of them, with either sign, for a. Each resolution of D thus gives rise to four ambiguous forms: but since $(c, 0, a) \backsim (a, 0, c)$, and we wish to find the number of ambiguous *classes*, we may reject two of the four, retaining those for which $|a| < |c|$. If n is the number of different primes which divide D, the number of forms which we obtain in this way is 2^n.

For example if $D = -90 = -2 . 3^2 . 5$, the forms are

$$(\pm 1, 0, \pm 90), \quad (\pm 2, 0, \pm 45), \quad (\pm 5, 0, \pm 18), \quad (\pm 9, 0, \pm 10):$$

that is 8 or 2^3 in all.

A properly primitive form $(2b, b, c)$ is obtained by taking for b any (positive or negative) divisor of D such that $c = (b^2 - D)/2b$ is an integer prime to $2b$. Now c being odd, $c^2 \equiv 1 \pmod 8$, and therefore

$$D = b^2 - 2bc = (b - c)^2 - c^2 \equiv 3 \pmod 4 \quad \text{or} \quad \equiv 0 \pmod 8,$$

according as b is odd or even. Hence D must be of the type $8n$, $8n + 3$, or $8n + 7$ if there are to be any forms of the kind now considered.

First suppose $D \equiv 3 \pmod 4$. Then if we take for b *any* divisor of D, b is necessarily odd, $b^2 - D \equiv 2 \pmod 4 \equiv 0 \pmod b$, so that c is certainly integral and odd: also $2c = b - D/b$, so that c is prime to b if, and only if, D/b is prime to b. Since b may be taken positively or negatively, we thus obtain $2 . 2^n = 2^{n+1}$ forms, n having the same meaning as before.

Next let $D \equiv 0 \pmod 8$, so that b must be even. Then since $2c = b - D/b$, we see that by dividing D into any two even factors b, D/b which have no common divisor except 2, c will be odd and prime to $\frac{1}{2}b$, and therefore also to $2b$. In this way we get altogether 2^{n+1} forms, allowing for variation of sign in b.

For instance let $D = 120 = 8 . 3 . 5$: the forms are

$$(\pm 4, \pm 2, \mp 29), (\pm 8, \pm 4, \mp 13), (\pm 12, \pm 6, \mp 7), (\pm 24, \pm 12, \pm 1),$$
$$(\pm 20, \pm 10, \mp 1), \quad (\pm 40, \pm 20, \pm 7), \quad (\pm 60, \pm 30, \pm 13),$$
$$(\pm 120, \pm 60, \pm 29):$$

in all $16 = 2^4$.

In every case the forms $(2b, b, c)$ may be arranged in pairs such as

$$(2b, b, c), \quad (2b', b', c),$$

where $$b' = 2c - b = -D/b.$$

Observing that $b + b' = 2c \equiv 0 \pmod{c}$,

we have
$$(2b,\, b,\, c) \sim (c,\, b',\, 2b') \sim (2b',\, -b',\, c)$$
$$\sim (2b',\, b',\, c),$$
so that we need only retain that form which has the smaller middle coefficient. Thus we have left 2^n forms $(2b, b, c)$, for which $|b| < |\sqrt{D}|$.

Now let μ denote the number of *odd* primes which divide D, so that $n = \mu$ or $\mu + 1$ according as D is odd or even; then the total number, N, of properly primitive ambiguous forms which we have retained (including both types when they exist) will be according to the following table.

$$\begin{array}{ll}
D \equiv 0 \pmod{8}, & N = 2 \,.\, 2^n = 2^{\mu+2}, \\
\;,, \equiv 4 \pmod{8}, & \;,, = 2^n \quad\;\; = 2^{\mu+1}, \\
\;,, \equiv 3 \pmod{4}, & \;,, = 2 \,.\, 2^n = 2^{\mu+1}, \\
\;,, \equiv 2 \pmod{4}, & \;,, = 2^n \quad\;\; = 2^{\mu+1}, \\
\;,, \equiv 1 \pmod{4}, & \;,, = 2^n \quad\;\; = 2^{\mu}.
\end{array}$$

Comparing this result with the scheme of generic characters (Art. 130) it appears that in every case *N is equal to the number of assignable total characters for the determinant D.*

157. In the case when D is negative, the forms retained will be half positive and half negative. We now reduce the system to one-half by rejecting all the negative forms. The $\frac{1}{2}N$ positive forms which remain all belong to distinct classes. For every form $(a, 0, c)$ is reduced, because $a < c$: and every form $(2b, b, c)$ is reduced unless $2b > c$, in which case the equivalent form $(c, c - b, c)$ is reduced, because $2b > c$ gives $c > 2(c - b)$, where observe that $c - b$ is positive, because b (which is positive) $< -D/b < 2c - b$, and therefore $2(c - b) > 0$.

No two of the reduced forms $(a, 0, c)$, $(2b, b, c)$, $(c, c - b, c)$ can be opposite or identical; so that, finally, the number of positive properly primitive ambiguous classes is $\frac{1}{2}N$.

Next, suppose that D is positive. Let (a, b, c) be any one of the N forms which have been retained. Choose b' so that
$$b' \equiv b \pmod{a}, \text{ and } 0 < \sqrt{D} - b' < |a|:$$
this can always be done, and in one way only.

Let $c' = (b'^2 - D)/a$: then (a, b', c') is equivalent to (a, b, c), and we can show that it is also reduced. The conditions for this are that $0 < b' < \sqrt{D}$ and $\sqrt{D} - b' < |a| < \sqrt{D} + b'$. Now if $|a| < \sqrt{D}$ it is clear from the conditions by which b' was determined that b' is positive and $< \sqrt{D}$, and since $|a| < \sqrt{D}$, *a fortiori* $|a| < \sqrt{D} + b'$, so that (a, b', c') is reduced. If $|a| > \sqrt{D}$, the form (a, b, c) must be of the type $(2b, b, c)$, where $|b| < \sqrt{D}$. Putting $b' = |b|$ we have $b' \equiv b \pmod{2b}$ while $0 < \sqrt{D} - b' < \sqrt{D} < |a|$: that is, $|b|$ satisfies the conditions which determine b'. Moreover

$$|a| = |2b| = 2|b| < \sqrt{D} + |b| < \sqrt{D} + b':$$

hence (a, b', c') is reduced.

In this way we replace every one of the N forms by an equivalent reduced ambiguous form; and these reduced forms are all different.

It can be proved that *every* reduced properly primitive ambiguous form will be found among the above set. For suppose (a, b, c) is any reduced properly primitive ambiguous form: then because it is reduced $0 < b < \sqrt{D}$, and hence if $b \equiv 0 \pmod{a}$, $|a| < \sqrt{D}$, and the form $(a, 0, c')$, equivalent to (a, b, c), is one of our original set, and hence (a, b, c) is the corresponding reduced form of the final set. If b is not divisible by a, a is even, and $(a, b, c) \backsim (a, \frac{1}{2}a, c')$: while, since for a reduced form $|a| < 2\sqrt{D}$, it follows that $\frac{1}{2}a$ divides D, and $|\frac{1}{2}a| < \sqrt{D}$, so that $(a, \frac{1}{2}a, c')$ is one of the original set, and therefore as before (a, b, c) is the corresponding reduced form.

Every ambiguous class contains two, and only two, reduced ambiguous forms; therefore, finally, the number of properly primitive ambiguous classes is $\frac{1}{2}N$.

158. *The number of improperly primitive ambiguous classes (when any exist) is equal to the number of properly primitive ambiguous classes of the same determinant.*

For let (a, b, c) be any properly primitive ambiguous form. Then if b is odd, a must be odd also: for if a were oddly even c would also be oddly even, because $D \equiv 1 \pmod{4}$, and the form would not be properly primitive. Hence $b \equiv 0 \pmod{a}$ and $c \equiv 0 \pmod{4}$. If b is even, a and c must both be odd: and the equivalent form $(a, a + b, c')$ comes under the preceding case. Thus when $D \equiv 1 \pmod{4}$ every properly primitive ambiguous class contains a form $(a, b, 4c)$ where a, b are odd and $b \equiv 0 \pmod{a}$.

This is one of the three forms derivable from the improperly primitive ambiguous form $(2a, b, 2c)$ by the reduced substitutions of order 2; therefore every properly primitive ambiguous class is connected with an improperly primitive one.

Now let $\phi = (2a, b, 2c)$ where $b \equiv 0 \pmod{a}$ be any improperly primitive ambiguous form;

$$\phi_1 = (a, b, 4c),$$
$$\phi_2 = (4a, b, c),$$
$$\phi_3 = (4a, 2a + b, a + b + c):$$

then ϕ_1 is properly primitive and ambiguous, and we have to prove that ϕ_2, ϕ_3 cannot belong to properly primitive and ambiguous classes except when $\phi_1 \backsim \phi_2 \backsim \phi_3$.

When $D \equiv 1 \pmod 8$, ϕ_2, ϕ_3 are not properly primitive (see Art. 153), and the theorem is proved. If $D \equiv 5 \pmod 8$ let

$$f_1 = (4, 1, \tfrac{1}{4}(1 - D)), \quad f_2 = (4, 3, \tfrac{1}{4}(9 - D)),$$

and let $\Phi_1, \Phi_2, \Phi_3, F_1, F_2$ be the classes containing $\phi_1, \phi_2, \phi_3, f_1, f_2$. Then it may be verified that

$$\Phi_2 = \Phi_1 F_1, \quad \Phi_3 = \Phi_1 F_2, \quad \text{or} \quad \Phi_2 = \Phi_1 F_2, \quad \Phi_3 = \Phi_1 F_1,$$

according as $b \equiv 1$ or $3 \pmod 4$.

Hence if Φ_2, Φ_3 are ambiguous classes, so must be F_1 and F_2.

Now $F_1^2 = F_2$, and $F_2^2 = F_1$: hence if F_1, F_2 are ambiguous, $F_1 = F_2 = 1$, and therefore $\phi_1 \backsim \phi_2 \backsim \phi_3$.

In every case, then, there is a (1, 1) correspondence between the properly and improperly primitive ambiguous classes, and therefore the number of classes of each kind is the same.

The method of this article is applicable to the more general problem of Art. 153. For in the general case, since ϕ_2 is compounded of ϕ_1 and either f_1 or f_2, it follows that if $\phi_2 \sim \phi_1$, either f_1 or f_2, and therefore also the other, must belong to the principal class; and also that if this is so, $\phi_1 \sim \phi_2 \sim \phi_3$.

Now it is easily found that $(1, 0, -D)$ is transformed into f_1 by the substitution

$$\begin{pmatrix} T, & \tfrac{1}{4}(T+DU) \\ U, & \tfrac{1}{4}(T+U) \end{pmatrix},$$

where $T^2 - DU^2 = 4$: and it can be proved as above (p. 168) that if (T, U) is any integral solution in which U is odd, we can choose the sign of U so as to make the substitution integral. This being done, the substitution

$$\begin{pmatrix} T, & \tfrac{1}{4}(3T-DU) \\ -U, & \tfrac{1}{4}(\ T-3U) \end{pmatrix},$$

is also integral and unitary, and transforms $(1, 0, -D)$ into f_2.

This is the point of view from which Gauss regards the correspondence between the properly and improperly primitive classes. (See *D. A.* Art. 256. VI.)

159. If K is a class of any actually existing genus, K^2 belongs to the principal genus. Let $K^2 = H$, and let $1, A_1, A_2 \ldots A_{k-1}$ be all the properly primitive ambiguous classes. Then H is produced by the duplication of $K, KA_1, KA_2 \ldots KA_{k-1}$, but by that of no other class. Hence if δ be the number of classes of the principal genus which can be produced by duplication, the total number of classes of which the duplicates belong to the principal genus is δk. But the duplicate of *every* class belongs to the principal genus. Therefore if g be the number of existing genera, ν the number of classes in each genus, $g\nu = k\delta$. Now δ cannot exceed ν: therefore g cannot exceed k: that is,

The number of actually existing genera cannot exceed that of the properly primitive ambiguous classes.

160. From this and Art. 157 we at once infer the impossibility of half the assignable generic characters, and this, it will be observed, independently of the law of quadratic reciprocity. We have, in fact, the material for a new and entirely different proof of that law: this is Gauss's 'demonstratio secunda,' (D. A. Art. 262).

We observe that when $D = -1, 2, -2$ or an odd prime $\pm p \equiv 1 \pmod 4$, there is only one genus, namely the principal genus: and that if $D = \pm pq \equiv 1 \pmod 4$, where p, q are primes, there cannot be more than two genera. The law of reciprocity is established by the following propositions:—

1. If a is any positive number of the form $4n + 3$, $-1Na$.

For if -1 were a residue of a, we could find integers b, c such that $-1 = b^2 - ac$, and then (a, b, c) would be a form of determinant -1 with the character $\chi = -1$, which is impossible.

2. If p is a prime and $\equiv 1 \pmod 4$, $-1Rp$.

For the form $(-1, 0, p)$ must belong to the principal genus for the determinant p (which is the only existing genus), and therefore $-1Rp$.

3. If p is a prime and $\equiv 1 \pmod 8$, both $+2$ and -2 are residues of p.

This follows from the consideration of the forms

$$(\pm 8, 1, \mp \tfrac{1}{8}(p-1)) \quad \text{or} \quad (\pm 8, 3, \mp \tfrac{1}{8}(p-9))$$

according as $p \equiv 9$ or $\equiv 1 \pmod{16}$. In either case we infer $\pm 8Rp$, and therefore $\pm 2Rp$.

4. If a is any number $\equiv 3$ or $5 \pmod 8$, $2Na$.

For otherwise we could find a form (a, b, c) of determinant 2, with the character $\psi = -1$.

5. If a is any number $\equiv 5$ or $7 \pmod 8$, $-2Na$.

For otherwise there would be a form (a, b, c) of determinant -2 with the character $\chi\psi = -1$.

6. If p is a prime, and $\equiv 3 \pmod 8$, $-2Rp$.

For, considering the generic characters for the determinant $2p$, the forms $(1, 0, -2p)$, $(-1, 0, 2p)$ show that these are $(n \mid p) = +1$, $\chi\psi = +1$, and $(n \mid p) = -1$, $\chi\psi = -1$. Now the form $(-2, 0, p)$ gives $\chi\psi = +1$, and therefore also $(-2 \mid p) = +1$, that is, $-2Rp$.

The theorem may also be proved by combining (1) and (4).

7. If p is prime and $\equiv 7 \pmod 8$, $2Rp$.

One of the forms $(8, 1, \frac{1}{8}(p+1))$, $(8, 3, \frac{1}{8}(p+q))$ of determinant $-p$, is properly primitive: and since there is only one genus, we infer $8Rp$ and therefore $2Rp$.

We might also combine (1) and (5).

8. Let p, q be two odd primes. Then first, if $p \equiv 1 \pmod 4$, and qNp, we shall have pNq. For otherwise we could find a form (q, b, c) of determinant p with the character $(n \mid p) = -1$.

Secondly, if $p \equiv 3 \pmod 4$, and qNp, then $-pNq$. For otherwise there would be a form (q, b, c) of determinant $-p$ with the character $(n \mid p) = -1$.

Thirdly, if $p \equiv 1 \pmod 4$ and qRp, then pRq. If $q \equiv 1 \pmod 4$ this follows from the first case, because pNq would involve qNp. If $q \equiv 3 \pmod 4$ then $-q \equiv 1 \pmod 4$ and $-qRp$, since $-1Rp$. Hence by the second case we infer pRq.

Lastly if $p \equiv 3 \pmod 4$, and qRp, then $-pRq$.

If $q \equiv 1 \pmod 4$ it follows from the first case that pRq, and therefore $-pRq$.

If $q \equiv 3 \pmod 4$, then the forms $(1, 0, -pq)$, $(-1, 0, pq)$ shew that the generic characters for the determinant pq are $(n \mid p) = +1$, $(n \mid q) = +1$, or else $(n \mid p) = -1$, $(n \mid q) = -1$. The form $(9, 0, -p)$ gives $(n \mid p) = +1$, and therefore $(-p \mid q) = +1$, that is, $-pRq$.

This completes the proof of the law of reciprocity.

161. It is a remarkable fact that *every* class of the principal genus may be obtained by duplication: that is to say, in our former notation (Art. 159), $\delta = \nu$, and therefore $g = k$. Two proofs of this important proposition will be given later on, one depending on the theory of ternary quadratic forms, and the other derived from Dirichlet's transcendental analysis. Meanwhile, the truth of the theorem will be assumed, for the purpose of giving a more complete account here than would otherwise be possible of the relations which connect the different classes in respect to composition.

Let H be any class of the principal genus, other than the principal class. Then since there are only ν distinct classes in the genus altogether, and since the $(\nu+1)$ classes H, H^2, $H^3 \ldots H^{\nu+1}$ all belong to it, at least two of them must be identical.

Suppose $H^\lambda = H^\mu$ where $\lambda > \mu$: then $H^{\lambda-\mu} = 1$, or $H^f = 1$ where f is a positive integer not greater than ν. Let f now denote the *least* positive integer such that $H^f = 1$: then f may be called the exponent to which the class H appertains: and the classes $1, H, H^2 \ldots H^{f-1}$ may be said to form a period.

Exactly as in the analogous theory of residues to a prime modulus (see Art. 18), it may be proved that f divides ν, so that every class of the principal genus satisfies the symbolical equation $H^\nu = 1$.

Again, the period of H^m will contain f/d terms, where $d = dv(m, f)$: in particular, if f is prime to m, it will contain f terms. If f is prime, the period of H^m will contain f terms, for all values of m.

162. If the principal genus contains a class G appertaining to the exponent ν, the determinant is said to be *regular*. In this case, the period of G comprises all the classes of the principal genus, and the class G enjoys properties similar to those of a primitive root of a prime modulus. For instance, taking G as a 'base,' any class of the principal genus may be specified by its index: there will be $\phi(\nu)$ classes such as G, any one of which may be taken for a base, etc. etc.

When the determinant is regular, the principal genus contains one or two ambiguous classes, according as ν is odd or even. For if G^m is ambiguous, $G^{2m} = 1$ and therefore $2m \equiv 0 \pmod{\nu}$: hence if ν is odd, the principal class is the only ambiguous class in the genus, while if ν is even, $G^{\nu/2}$ is also ambiguous.

If, then, the principal genus contains more than two ambiguous classes, the determinant is certainly irregular. This consideration enables us to discover irregular determinants. For instance, the three primes 3, 13, 61 are such that each is a quadratic residue of each of the other two; and the determinant $-2379 = -3.13.61$ is irregular, because the principal genus contains, besides the principal class, the three ambiguous classes $(3, 0, 793)$, $(39, 0, 61)$, $(13, 0, 183)$.

163. It may also be shewn that every negative determinant of the form $-(8km+3)m^2$, when k is any positive integer (not zero), and m any odd positive integer greater than 1, is irregular. For let $f_1 = (m^2, m, 8km+4)$, $f_2 = (4m^2, m, 2km+1)$, and let K_1, K_2 be the classes to which f_1 and f_2 belong. Then K_1 and K_2 are properly primitive classes of the principal genus, and it can be shewn by Arndt's formulæ of composition (Art. 142 above), that $K_1^2 = K_1^{-1}$, and $K_2^2 = K_2^{-1}$, whence also $K_1^3 = K_2^3 = 1$.

Moreover f_1 and f_2 belong to different classes: for either f_1 or the adjacent form $(8km+4, -m, m^2)$ is reduced; and similarly either f_2 or its equivalent $(2km+1, -m, 4m^2)$ is reduced; the two reduced forms are in no case equivalent, and neither of them is the principal form.

We thus obtain three distinct periods of three terms

$$(1, K_1, K_1^2),\quad (1, K_2, K_2^2),\quad (1, K_1^2K_2, K_1K_2^2).$$

But, in the case of a regular determinant, a period of three terms can only occur when ν is divisible by 3; and even when this is the case there is only *one* such period, namely $(1, G^{\nu/3}, G^{2\nu/3})$ where G is a base of the period of principal classes. The determinant considered is therefore irregular.

We see, then, that an infinite number of irregular determinants may be found; it should be observed, however, that we cannot obtain, in either of the ways just explained, all the irregular determinants which exist: thus there are prime irregular determinants, such as -307. It does not appear to be possible to find a general formula which will apply to all cases.

164. Returning to the case of a regular determinant, suppose that G is any class whose period comprises all the classes of the principal genus: then, by the theorem which, for the present, we are anticipating, there is a class H such that $G = H^2$. If ν is odd, we may evidently put $H = G^{\frac{1}{2}(\nu+1)}$, and in fact this proves the theorem about duplication for this special case. The principal genus $(1, G, G^2, \ldots G^{\nu-1})$ contains only one ambiguous class: and if A_1, $A_2 \ldots A_{k-1}$ are the other ambiguous classes, the remaining genera will be

$$(A_1, A_1G, A_1G^2 \ldots A_1G^{\nu-1}),$$

$$(A_2, A_2G \ldots A_2G^{\nu-1}) \ldots (A_{k-1}, A_{k-1}G \ldots A_{k-1}G^{\nu-1}).$$

Next suppose that ν is even. In this case H cannot belong to the principal genus; for if it did, we should have $H = G^m$ and $G^{2m-1} = 1$, which is impossible. There will therefore be two associated genera, the principal genus

$$(1, H^2, H^4 \ldots H^{2\nu-2}),$$

and

$$(H, H^3, H^5 \ldots H^{2\nu-1}).$$

If C is a class of any other existing genus, all the classes of that genus will be given by

$$(C, CH^2, CH^4 \ldots CH^{2\nu-2}),$$

and there will be an associated genus

$$(CH, CH^3 \ldots CH^{2\nu-1}).$$

It is also evident that every genus contains either two ambiguous classes or none: viz. if any genus contains an ambiguous class A, it will also contain AH^ν and no others. Half of the existing genera will contain no ambiguous classes.

We may, if we please, adopt a similar arrangement when ν is odd, by putting $H = AG^{\frac{1}{2}(\nu+1)}$, A being any ambiguous class, not the principal class. Thus in all cases we have a class H with 2ν terms in its period; and the genera arranged in corresponding pairs

$$(A, AH^2, AH^4, \ldots AH^{2\nu-2}), \quad (AH, AH^3, \ldots AH^{2\nu-1}),$$

where A is ambiguous: each ambiguous genus being associated with one that is non-ambiguous, or ambiguous, according as ν is even or odd.

165. In illustration, we give the complete tabulation of the primitive classes for $D = -365$. There are four genera, each containing five classes: so that both modes of arrangement are possible.

		Characters			Comp.	
		$\left(\frac{n}{5}\right)$	$\left(\frac{n}{73}\right)$	χ	(i).	(ii).
I.	$(1,\ 0,\ 365)$	+	+	+	1	1
	$(6,\ 1,\ 61)$				f^2	g
	$(9,\ -2,\ 41)$				f^4	g^2
	$(9,\ 2,\ 41)$				f^6	g^3
	$(6,\ -1,\ 61)$				f^8	g^4
II.	$(11,\ 3,\ 34)$	+	−	−	f	a_1g^3
	$(15,\ 5,\ 26)$				f^3	a_1g^4
	$(10,\ 5,\ 39)$				f^5	a_1
	$(15,\ -5,\ 26)$				f^7	a_1g
	$(11,\ -3,\ 34)$				f^9	a_1g^2
III.	$(2,\ 1,\ 183)$	−	+	−	a	a_2
	$(3,\ 1,\ 122)$				af^2	a_2g
	$(18,\ 7,\ 23)$				af^4	a_2g^2
	$(18,\ -7,\ 23)$				af^6	a_2g^3
	$(3,\ -1,\ 122)$				af^8	a_2g^4
IV.	$(17,\ -3,\ 22)$	−	−	+	af	a_3g^3
	$(13,\ -5,\ 30)$				af^3	a_3g^4
	$(5,\ 0,\ 73)$				af^5	a_3
	$(13,\ 5,\ 30)$				af^7	a_3g
	$(17,\ 3,\ 22)$				af^9	a_3g^2.

166. When the determinant is irregular, the classes of the principal genus cannot be arranged in one period; it will be possible, however, to assign a certain number of bases such that all the classes of the genus are expressible by powers and products of powers of these bases: and any particular class may then be specified by means of two or more indices.

Suppose that g is the highest exponent to which any class of the principal genus appertains: then the exponent belonging to any class of the genus will divide g. This is proved by shewing (compare Art. 20) that if H, K appertain to the exponents e, f, HK will appertain to the exponent μ, where μ is the least common multiple of e and f.

Again g divides ν, the number of classes in the genus. For if

1, G, $G^2 \dots G^{g-1}$ be any period of g terms, then the classes of the genus may be arranged in sets such as C, CG, $CG^2 \dots CG^{g-1}$, no two of which have a class in common.

The quotient ν/g is called by Gauss the exponent of irregularity. In Gauss's tables relating to definite forms, which include more than 4,900 negative determinants, the only exponents of irregularity which occur are 2 and 3, with one exception,

$$D = -11907,$$

for which it is 9. According to Pepin, the exponent is also 9 for $D = -6075$.

For further details, especially with regard to the choice of bases for irregular determinants, and the arrangement of classes not contained in the principal genus, the reader is referred to Smith's *Report*, Arts. 118, 119.

AUTHORITIES.

GAUSS: *D. A.* Arts. 234—265.

Démonstration de quelques théorèmes concernant les périodes des classes des formes binaires du second degré (Werke, ii. 266).

Tafel der Anzahl der Classen binärer quadratischer Formen (Werke, ii. 449), with notes and corrections by Schering (ibid. p. 521).

SMITH, H. J. S. Report on the Theory of Numbers, Part IV. (Report of British Ass. 1862).

DIRICHLET-DEDEKIND: Vorlesungen über Zahlentheorie (3rd edition 1879) Supplement X. See also Dirichlet: *De formarum binariarum secundi gradus compositione* (Crelle, xlvii. (1854) p. 155).

ARNDT, F.: *Auflösung einer Aufgabe in der Composition der quadratischen Formen* (Crelle, lvi. (1859) p. 64).

Ueber die Anzahl der Genera der quadratischen Formen (ibid. p. 72).

LIPSCHITZ, R.: *Einige Sätze aus der Theorie der quadratischen Formen* (Crelle, liii. (1857) p. 238).

SCHERING, E.: *Die Fundamental-Classen der zusammensetzbaren arithmetischen Formen* (Göttingen 1869). Also in vol. xiv. of the Abhandl. d. königl. Gesellsch. d. Wiss. zu Göttingen.

POINCARÉ, H.: *Sur un mode nouveau de représentation géométrique des formes quadratiques définies ou indéfinies.* (Journ. de l'École Polytechnique, cah. 47, t. xxviii. (1880) p. 177.) See especially pp. 226 and following.

The theory of composition, as now understood, is principally due to Gauss. Some special cases of composition were discovered previously, such as

$$(x^2+y^2)(x'^2+y'^2) = (xx'-yy')^2 + (xy'+x'y)^2,$$

with the analogous theorem of Euler's for the product of sums of four squares

The most interesting of these earlier results will be found in Lagrange's memoir *Sur la solution des problèmes indéterminés du second degré* (Hist. de l'Acad. de Berlin 1767) § VI. Lagrange demonstrates a general theorem, which is equivalent to what would now be called the duplication of the form

$$\Pi\,(x_1+x_2\theta+x_3\theta^2+\ldots+x_n\theta^{n-1}),$$

where $x_1, x_2,\ldots x_n$ are the variables, and the product sign extends over all values of θ for which $\theta^n-A=0$, A being any integer. See also the additions to Euler's Algebra, § 9.

In Vol. LX. of Crelle's Journal (1862) p. 357 there is a table, calculated by Cayley, which gives the complete classification of primitive binary quadratic forms for negative determinants from $D=-1$ to $D=-100$, and for positive determinants, other than squares, from $D=2$ to $D=99$. The generic characters are also given, and the composition of the different classes is indicated by symbols as on p. 181 above. The table also contains the periods of reduced forms for the positive determinants. There is a supplementary table relating to the thirteen irregular negative determinants which are numerically less than 1000.

CHAPTER VII.

Cyclotomy.

167. THE theory of indices and power-residues cannot have failed to remind the reader of the binomial equation $x^m - 1 = 0$, upon which depends the division of the period of the circular functions. The analogy is by no means accidental, and there are, in fact, many arithmetical results which are most simply expressed, and most easily proved, with the aid of the complex roots of unity; moreover, as Gauss first pointed out, the problem of cyclotomy, or division of the circle into a number of equal parts, depends in a very remarkable way upon arithmetical considerations. We have here the earliest and simplest example of those relations of the theory of numbers to transcendental analysis, and even to pure geometry, which so often unexpectedly present themselves, and which, at first sight, are so mysterious.

168. The equation $x^m - 1 = 0$ has m roots, of which only one is real, namely 1. Expressed in terms of circular functions, the roots are given by

$$x_h = \cos\frac{2h\pi}{m} + i\sin\frac{2h\pi}{m} = e^{2h\pi i/m}$$

$$(h = 0,\ 1,\ 2 \ldots \overline{m-1}).$$

From this, and de Moivre's theorem, the propositions which immediately follow may be deduced without any difficulty; in order, however, to preserve, as far as possible, the analogy with binomial congruences, they will be proved independently.

If α is any root of $x^m - 1 = 0$, and e is any integer, α^e is also a root, because $(\alpha^e)^m = (\alpha^m)^e = 1^e = 1$.

Let f be the least positive integral exponent (not zero) such that $\alpha^f = 1$. Since $\alpha^m = 1$, it is clear that such an exponent must exist, and cannot exceed m. It is called the exponent to which α appertains. The root 1 appertains to the exponent 1, and is the only one of the kind.

The quantities $1, \alpha, \alpha^2, \ldots \alpha^{f-1}$, where α, f have the same meanings as before, are all roots of $x^m - 1 = 0$. Moreover they are all different, because if we had $\alpha^p = \alpha^q$ with $p < f$ and $q < f$, it would follow that $\alpha^{p \sim q} = 1$, or $\alpha^{f'} = 1$, with $f' < f$, which is impossible.

The exponent f is a divisor of m. For if not, let

$$dv(m, f) = \delta < f,$$

and choose integers p, q such that $pm + qf = \delta$; then

$$\alpha^\delta = (\alpha^m)^p (\alpha^f)^q = 1,$$

where $\delta < f$, contrary to the condition by which f is defined.

Let $1, a, b, c \ldots l$ be the $\phi(f)$ numbers which are less than f and prime to it; then the quantities

$$\alpha, \alpha^a, \alpha^b, \alpha^c, \ldots \alpha^l$$

are all different and all appertain to the exponent f. The proof of this is exactly similar to that of Art. 19.

In particular, there are $\phi(m)$ roots of $x^m - 1 = 0$ which appertain to the exponent m. These are called primitive mth roots of unity.

All the roots of $x^m - 1 = 0$ may be arranged into groups, each group consisting of the $\phi(f)$ roots appertaining to the exponent f, where f is any divisor of m.

It follows that the problem of finding all the roots of $x^m - 1 = 0$ is the same as that of finding all the *primitive* roots of

$$x^m - 1 = 0, \; x^d - 1 = 0, \; x^{d'} - 1 = 0, \text{ etc.}$$

where m, d, d', etc. are the different divisors of m, unity and m inclusive.

169. Let m and n be any positive integers prime to each other; then if α, β are primitive roots of $x^m - 1 = 0$ and $x^n - 1 = 0$ respectively, $\alpha\beta$ is a primitive root of $x^{mn} - 1 = 0$.

For suppose, if possible, that $\alpha\beta$ appertains to the exponent d, so that

$$(\alpha\beta)^d - 1 = 0$$

with $d < mn$. Then since $(\alpha\beta)^{mn} - 1 = 0$, d must divide mn, and hence $d = m'n'$, where m', n' divide m, n respectively.

Suppose that $m' < m$, and put $k = n/n'$, which is an integer. Then

$$1 = (\alpha\beta)^{dk} = \alpha^{m'n}\beta^{m'n}$$
$$= \alpha^{m'n},$$

since $\beta^n = 1$. Now $dv(m, m'n) = m'$, so that we can find integers x, y such that

$$xm'n + ym = m' ;$$

and hence
$$\alpha^{m'} = (\alpha^{m'n})^x (\alpha^m)^y = 1,$$

with $m' < m$; but this is impossible. Similarly the hypothesis $n' < n$ leads to $\beta^{n'} = 1$, which is impossible; therefore $m' = m$, $n' = n$, $d = mn$, and the proposition is proved.

By the repeated application of this theorem, the discovery of the primitive roots of $x^m - 1 = 0$, where $m = p^a q^b r^c \ldots$ is made to depend upon finding the primitive roots of $x^{p^a} - 1 = 0$, $x^{q^b} - 1 = 0$, etc.; $p, q, r \ldots$ being the different prime factors of m.

170. For the present, we shall suppose that m is an odd prime, p, so that the equation considered is

$$x^p - 1 = 0.$$

This has p roots, of which $(p-1)$ are primitive and satisfy the equation

$$X_p = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \ldots + x + 1 = 0.$$

When there is no risk of ambiguity, X will be used instead of X_p to denote the polynomial $(x^p - 1)/(x - 1)$.

If r is any root of $X = 0$, then all its roots are given by $r, r^2, r^3, \ldots r^{p-1}$. The equation is therefore of the type discussed by Abel in his *Mémoire sur une classe particulière d'équations résolubles algébriquement* (Crelle iv. (1829), p. 131), all the roots being expressible as rational functions of any one of them. It is, so to speak, the normal form of Abelian equation with real integral coefficients; the roots of all such equations, according to Kronecker, being expressible as rational functions of complex roots of unity. (See Serret, *Algèbre Supérieure* (4th ed.) ii. p. 684.)

171. The polynomial X is *irreducible*, in the sense that it cannot be expressed as the product of two polynomials of lower degree with rational coefficients.

Many proofs of this very important proposition have been given; the one which will be adopted here is due to Eisenstein (Crelle

xxxix. (1850), p. 166). Before giving it, however, it will be necessary to prove a lemma which was first enunciated by Gauss. (*D.A.* Art. 42.)

The lemma is as follows:

Let $F(x)=x^p+a_1x^{p-1}+a_2x^{p-2}+\ldots+a_p$ be a polynomial in x with integral coefficients, the coefficient of the highest power of x being unity: then, if $F(x)$ can be expressed as the product of two other polynomials

$$f(x)=x^m+b_1x^{m-1}+b_2x^{m-2}+\ldots+b_m,$$
$$\phi(x)=x^n+c_1x^{n-1}+c_2x^{n-2}+\ldots+c_n,$$

where $m+n=p$, and the coefficients are rational, these coefficients b_i, c_i must also be integral.

We may suppose that b_i, c_i are reduced to their lowest terms. Assuming that they are not integral, let p be a prime which occurs in any of the denominators; then among the coefficients b_i there will be one, say b_h, the denominator of which contains p to a higher power than the denominator of any of the preceding coefficients $b_1, b_2, \ldots b_{h-1}$, and to at least as high a power as any of the following denominators; and similarly among the coefficients c_i there will be one, say c_k, the denominator of which involves a higher power of p than the denominator of any of the preceding, and at least as high a power as any of those which follow. It may happen that p does not occur at all in the denominators of the b_i; in this case we put $b_h=1$, and in the same way we may have to put $c_k=1$, but we cannot have $b_h=1$ and $c_k=1$ simultaneously. Hence we may write

$$b_h=\frac{e}{fp^\alpha}, \qquad c_k=\frac{e'}{f'p^\beta},$$

where $\alpha+\beta \nless 1$, and e, f, e', f' are integers prime to p.

Now the coefficient of x^{n-h-k} in the product of $f(x)$ and $\phi(x)$ is equal to

$$b_hc_k+b_{h+1}c_{k-1}+b_{h+2}c_{k-2}+\ldots$$
$$+b_{h-1}c_{k+1}+b_{h-2}c_{k+2}+\ldots$$

The first term of this expression is $ee'/ff'p^{\alpha+\beta}$, and the denominators of the other terms cannot involve p to so high a power as $p^{\alpha+\beta}$; hence the sum of all the terms must be of the form

$$\frac{P+Qp^\gamma}{Rp^{\alpha+\beta}},$$

where P, R are integers prime to p, and γ is a positive integer at least equal to 1. This expression is necessarily a fraction, because p is a factor of the denominator, and the numerator is prime to p. This is inconsistent with the assumption that the coefficients of $f\phi$ or F are all integral: and the lemma is therefore proved.

Eisenstein's proof of the irreducibility of X depends on the following proposition:—

If p is a prime number, the polynomial $f(x)$ is irreducible if the coefficient of the highest power of x is unity, the absolute term $\pm p$, and all the other coefficients divisible by p.

It is clear that if $f(x)$ can be resolved into the product of two polynomials with rational, and therefore integral coefficients, we must have

$$f(x) = (x^m + b_1x^{m-1} + \dots + b_{m-1}x \pm 1)(x^n + c_1x^{n-1} + \dots + c_{n-1}x \pm p).$$

The coefficient of x on the right hand is

$$\pm c_{n-1} \pm pb_{m-1},$$

and since this is divisible by p, we have $c_{n-1} \equiv 0 \pmod{p}$. The coefficient of x^2 is

$$\pm c_{n-2} + c_{n-1}b_{m-1} \pm pb_{m-2},$$

and from this we infer that $c_{n-2} \equiv 0 \pmod{p}$. Proceeding in this way, we find that all the coefficients $c_1, c_2, \dots c_{n-1}$ are divisible by p; hence the coefficient of x^n on the right-hand side of the assumed identity is

$$\pm 1 + c_1b_{m-1} + c_2b_{m-2} + \dots \equiv \pm 1 \pmod{p};$$

but this contradicts the hypothesis that it is divisible by p. The assumed resolution into factors is therefore impossible.

To apply this to the polynomial X, we first transform it by changing x into $x+1$; it is obvious that if the new polynomial X' is irreducible, so also is X. Now the value of X' is

$$\frac{(x+1)^p - 1}{(x+1) - 1} = x^{p-1} + px^{p-2} + \frac{p(p-1)}{2}x^{p-3} + \dots + p,$$

the coefficients being those of the binomial expansion $(1+x)^p$.

All the coefficients except the first are divisible by p, so that X' satisfies the conditions laid down in the preceding proposition; hence X', and therefore also X, is irreducible.

172. Let r be any root of the equation $X=0$; then every rational integral function of r with rational coefficients may be reduced, without altering its value, to the form

$$c_0+c_1r+c_2r^2+\ldots+c_{p-2}r^{p-2}.$$

For suppose that $F(r)$ is any rational integral function of r, the degree of which exceeds $(p-2)$. By the process of algebraical division we can establish the identity

$$F(x)=QX+R,$$

where the degree of R is less than $(p-1)$. Putting $x=r$, we have $F(r)=$ the value of R when $x=r$; and this is an expression of the form given above.

Since the coefficient of the highest power of x in X is unity, it follows that if the coefficients of $F(r)$ are all integers, the coefficients c_0, c_1, etc. will also be integers.

The reduction thus effected is unique. For if we put

$$c_0+c_1r+c_2r^2+\ldots+c_{p-2}r^{p-2}=c_0'+c_1'r+c_2'r^2+\ldots+c'_{p-2}r^{p-2},$$

so that $(c_0-c_0')+(c_1-c_1')\,r+\ldots+(c_{p-2}-c'_{p-2})\,r^{p-2}=0,$

we must have

$$c_0-c_0'=c_1-c_1'=\ldots=c_{p-2}-c'_{p-2}=0;$$

because otherwise r would satisfy an equation, with rational coefficients, of lower degree than $p-1$; this is impossible, since X is irreducible.

The simplest way of making the reduction is to substitute for every term r^h its equivalent $r^{h'}$, where h' is the least positive residue of h to modulus p; if, after this, there are any terms in r^{p-1}, we replace r^{p-1} by the equivalent expression

$$-(r^{p-2}+r^{p-3}+\ldots+r+1).$$

More generally let

$$f(r)=\frac{\phi(r)}{\psi(r)}$$

be any rational function of r; $\phi(r)$, $\psi(r)$ being polynomials in r. Then we have identically

$$f(r)=\frac{\phi(r)\,.\,\psi(r^2)\,.\,\psi(r^3)\ldots\psi(r^{p-1})}{\psi(r)\,.\,\psi(r^2)\,.\,\psi(r^3)\ldots\psi(r^{p-1})}.$$

Now the denominator is a symmetric function of the roots of $X=0$, and may therefore be expressed in a form which is independent of r; the numerator is a rational integral function of r, and may therefore be reduced as above. Finally we obtain $f(r)$ in the form

$$f(r) = c_0 + c_1 r + c_2 r^2 + \dots + c_{p-2} r^{p-2},$$

where the coefficients, however, will not generally be integers. If the coefficients of $\psi(r)$ are integers, the product

$$\psi(r)\,\psi(r^2)\dots\psi(r^{p-1})$$

is a real integer N; and if the coefficients of $\phi(r)$ are also integers, then $c_0, c_1, \dots c_{p-2}$ will be rational fractions, the denominators of which are divisors of N.

In relation to the equation $X = 0$ the quantities

$$\psi(r),\ \psi(r^2), \dots \psi(r^{p-1})$$

are said to be *conjugate*; and the expression

$$N = \psi(r) \,.\, \psi(r^2) \dots \psi(r^{p-1})$$

is called the *norm* of $\psi(r)$ and written $\mathrm{Nm} \,.\, \psi(r)$. These definitions must not be confounded with those of Art. 94.

173. We shall now give an account of Gauss's theory of the algebraical solution of $X = 0$; but before doing so, it seems desirable to explain the precise object of the investigation. So far as notation goes, the simplest way of expressing the solution is to say that the roots of $X = 0$ are all the values of $1^{1/p}$ except 1; and in a certain sense this is also the theoretically simplest form of the solution. But if we classify algebraical functions according to the character of the irrationalities which they *necessarily* involve, the matter is quite different. Thus, for instance, when $p = 5$, the equation $X = 0$ is

$$x^4 + x^3 + x^2 + x + 1 = 0,$$

and if we put $x + x^{-1} = y$ this becomes

$$y^2 + y - 1 = 0;$$

the roots of which are

$$y_1 = \frac{-1 + \sqrt{5}}{2}, \qquad y_2 = \frac{-1 - \sqrt{5}}{2}.$$

Hence the four values of x are obtained by solving the two quadratics

$$x^2 - y_1 x + 1 = 0, \qquad x^2 - y_2 x + 1 = 0;$$

whence

$$x = \frac{-1 \pm \sqrt{5} + \sqrt{-10 \mp 2\sqrt{5}}}{4}, \text{ or } \frac{-1 \pm \sqrt{5} - \sqrt{-10 \mp 2\sqrt{5}}}{4};$$

and although these expressions are more complicated than $1^{1/5}$, of which they are values, still they are to be considered more simple in so far as they do not involve the extraction of any higher root than the second; and from this point of view the reduction of the solution of $(x^5-1)/(x-1)=0$ to that of a set of quadratic equations is to be regarded as an essential simplification.

In a similar way it can be shewn by Gauss's method that, in the general case when p is any odd prime, the solution of $X_p=0$ may be made to depend upon a system of auxiliary equations, the character of which is essentially connected with the resolution of $(p-1)$ into its prime factors. In particular, if p is a prime of the form 2^n+1, such as 3, 5, 17, 257, etc., the simplest auxiliary system is composed entirely of *quadratic* equations; and since quadratic equations may be graphically solved by the constructions of Euclid's *Elements*, the remarkable conclusion follows that regular polygons of 3, 5, 17, 257, ... sides may be constructed by Euclidean methods.

174. The whole investigation is based upon a peculiar method of grouping the roots of $X=0$. It has already appeared (Art. 170) that if r is any one of the roots, then the whole set of $(p-1)$ roots is given by $r, r^2, r^3, \dots r^{p-1}$. Now let g be a primitive root of the congruence $x^{p-1}-1\equiv 0 \pmod{p}$; then the roots of $X=0$ may be equally well represented by

$$r,\ r^g,\ r^{g^2},\ r^{g^3},\dots r^{g^{p-2}},$$

r, as before, denoting any one of the roots.

Let $p-1=ef$ be any resolution of $(p-1)$ into two factors, and write

$$\begin{aligned}
\eta_0 &= r + r^{g^e} + r^{g^{2e}} + \dots + r^{g^{(f-1)e}},\\
\eta_1 &= r^g + r^{g^{e+1}} + r^{g^{2e+1}} + \dots + r^{g^{(f-1)e+1}},\\
&\vdots\\
\eta_k &= r^{g^k} + r^{g^{e+k}} + r^{g^{e+k}} + \dots + r^{g^{(f-1)e+k}},\\
&\vdots\\
\eta_{e-1} &= r^{g^{e-1}} + r^{g^{2e-1}} + r^{g^{3e-1}} + \dots + r^{g^{fe-1}}
\end{aligned}$$

These quantities will be called the f-nomial periods of the roots. If we change r into r^m, η_k is transformed into η_{k+i} where $i=\operatorname{ind}_g m$; that is to say, we produce a cyclical permutation of the periods. The particular period denoted by η_k will depend upon the choice of g, as well as upon that of r; but it is easily seen that in every case we have the same set of periods, only in a different order.

As a matter of convenience, we may extend the notation of the periods by allowing the suffixes to assume all integral values whatever. The equations defining the periods will remain just the same, and we shall have $\eta_{k'} = \eta_k$ if $k' \equiv k \pmod{e}$.

Of course, in the practical calculation of the periods, the exponents of the different powers of r may be reduced to their least residues (mod p).

Example. Suppose $p = 13$, $e = 4$, $f = 3$.

Taking $g = 2$, we have the four periods

$$\begin{aligned}\eta_0 &= r + r^3 + r^9,\\ \eta_1 &= r^2 + r^5 + r^6,\\ \eta_2 &= r^4 + r^{10} + r^{12},\\ \eta_3 &= r^7 + r^8 + r^{11}.\end{aligned}$$

If $g = 6$, the periods are the same, in the same order; if we take $g = 7$ or 11, they are

$$\eta_0' = \eta_0, \quad \eta_1' = \eta_3, \quad \eta_2' = \eta_2, \quad \eta_3' = \eta_3.$$

175. If in the expression for η_k we change r into r^{g^e}, the value of η_k is not altered; all that happens is that the terms which compose it are cyclically interchanged. With this fact is connected the important proposition that

Every rational function of r which remains unaltered when r is changed into r^{g^e} may be expressed as a linear function of the f-nomial periods.

By Arts. 172, 174 we may suppose the given rational function of r reduced to the form

$$\phi(r) = a_0 r + a_1 r^g + a_2 r^{g^2} + \dots + a_{p-2} r^{g^{p-2}}$$

where $a_0, a_1, \dots a_{p-2}$ are independent of r.

Change r successively into $r^{g^e}, r^{g^{2e}}, \dots r^{g^{(f-1)e}}$: each of these substitutions leaves $\phi(r)$ unaltered: therefore

$$\begin{aligned}\phi(r) &= a_0 r^{g^e} + a_1 r^{g^{e+1}} + a_2 r^{g^{e+2}} + \dots\\ &= a_0 r^{g^{2e}} + a_1 r^{g^{2e+1}} + a_2 r^{g^{2e+2}} + \dots\\ &\;\vdots\\ &= a_0 r^{g^{(f-1)e}} + a_1 r^{g^{(f-1)e+1}} + \dots.\end{aligned}$$

Hence, by addition,

$$\begin{aligned} f\cdot\phi(r) &= a_0\eta_0 + a_1\eta_1 + \ldots + a_{p-2}\,\eta_{p-2} \\ &= (a_0 + a_e + a_{2e} + \ldots + a_{fe})\,\eta_0 \\ &+ (a_1 + a_{e+1} + a_{2e+1} + \ldots + a_{(f-1)e+1})\,\eta_1 \\ &+ \ldots \\ &+ (a_{e-1} + a_{2e-1} + \ldots + a_{fe-1})\,\eta_{e-1} \end{aligned}$$

and the proposition is proved.

If the coefficients a_0, a_1, etc. are rational, we have

$$\phi(r) = b_0\eta_0 + b_1\eta_1 + \ldots + b_{e-1}\,\eta_{e-1}$$

where b_0, b_1, etc. are rational: and if the coefficients a_i are integers, the coefficients b_i must be integers also, because each power of r occurs in only one of the periods and then with a coefficient 1. In fact, we have in this case

$$\begin{aligned} b_0 &= a_0 = a_e = \ldots = a_{fe}, \\ b_1 &= a_1 = a_{e+1} = \ldots = a_{(f-1)e+1}, \end{aligned}$$

and so on.

Exactly as in Art. 172, it may be proved that the reduction is unique, and, in general, that a relation

$$a_0\eta_0 + a_1\eta_1 + \ldots + a_{e-1}\,\eta_{e-1} = b_0\eta_0 + b_1\eta_1 + \ldots + b_{e-1}\,\eta_{e-1},$$

with coefficients a_i, b_i independent of r, implies that $a_i = b_i$; because if we substitute for the periods their expressions in terms of r, and then divide both sides of the given relation by r, we obtain an equation satisfied by r the degree of which does not exceed $(p-2)$; this can only be if the equation reduces to an identity.

176. It follows immediately from the theorem of last article that every rational function of the periods may be expressed as a linear homogeneous function of them; and, in particular, that every rational integral function of the periods with integral coefficients may be expressed as a linear homogeneous function of the periods with integral coefficients.

In the practical application of this theorem it is useful to remember that $\Sigma\eta_i = r + r^2 + \ldots r^{p-1} = -1$.

As an illustration, let us take the example of Art. 174, in which $p = 13$,

$$\eta_0 = r + r^3 + r^9, \qquad \eta_2 = r^4 + r^{10} + r^{12},$$
$$\eta_1 = r^2 + r^5 + r^6, \qquad \eta_3 = r^7 + r^8 + r^{11}.$$

We have here, for instance,

$$\eta_0^2 = r^2 + 2r^4 + r^6 + 2r^{10} + 2r^{12} + r^5 = \eta_1 + 2\eta_2,$$

$$\eta_0\eta_2 = \eta_1 + \eta_3 + 3 = -3\eta_0 - 2\eta_1 - 3\eta_2 - 2\eta_3,$$

and so on.

177. *Every rational symmetric function of the periods with rational coefficients is a rational number.*

Let S be the given symmetric function; then it may be reduced to the form

$$S = a_0\eta_0 + a_1\eta_1 + \ldots + a_{e-1}\eta_{e-1}$$

where $a_0, a_1, \ldots a_{e-1}$ are rational. Since S is not affected by cyclical permutation of the periods,

$$\begin{aligned} S &= a_0\eta_1 \ + a_1\eta_2 + \ldots + a_{e-1}\eta_0 \\ &= a_0\eta_2 \ + a_1\eta_3 + \ldots + a_{e-1}\eta_1 \\ &= \ldots \\ &= a_0\eta_{e-1} + a_1\eta_0 + \ldots + a_{e-1}\eta_{e-2}. \end{aligned}$$

Therefore, by addition,

$$eS = \Sigma a_i \Sigma \eta_i = -\Sigma a_i$$

and S is a rational number. It is, in fact, obvious enough that $S = -a_0 = -a_1 = \ldots = -a_{e-1}$.

In particular, the elementary symmetric functions of the periods, that is to say, $\Sigma\eta_i$, $\Sigma\eta_i\eta_k$, etc. are rational integers. Therefore the periods $\eta_0, \eta_1, \ldots \eta_{e-1}$ are the roots of an equation

$$F(\eta) = 0$$

of degree e and with integral coefficients: the coefficient of η^e being unity.

The polynomial $F(\eta)$ is irreducible, in the sense that it cannot be resolved into the product of two integral functions of η of lower degree with rational coefficients. For suppose, if possible, that $F(\eta) = \phi(\eta).\psi(\eta)$: then the equation $\phi(\eta) = 0$ is satisfied by a certain number of the periods, say $\eta_\alpha, \eta_\beta, \ldots \eta_\lambda$, and we may suppose that none of these periods involves r^{p-1}, because, if r^{p-1} did occur, we could take $\psi(\eta)$ instead of $\phi(\eta)$. Let

$$\phi(\eta) = \eta^m + a\eta^{m-1} + \ldots;$$

then, by supposition, a is rational, and therefore integral (Art. 171), and we have

$$\eta_\alpha + \eta_\beta + \ldots + \eta_\lambda + a = 0;$$

but if η_α, η_β, etc. are expressed in terms of r this is an equation in r with integral coefficients and of degree less than $(p-1)$, and by Art. 171 this cannot possibly be satisfied.

The same result may also be very easily deduced from the last paragraph of Art. 175.

178. The most direct way of forming the equation $F(\eta)=0$ is by actually calculating the values of the symmetric functions $\Sigma\eta_i$, $\Sigma\eta_i\eta_k$, $\Sigma\eta_i\eta_k\eta_l$, etc. which are the coefficients of $F(\eta)$. Practically, however, it is more convenient to proceed as follows.

Let η be any one of the periods: then, by Art. 176, we can express $\eta\eta_0, \eta\eta_1, \eta\eta_2, \ldots \eta\eta_{e-1}$ as linear functions of the periods, so that

$$\begin{aligned}
\eta\eta_0 &= a_0\eta_0 + a_1\eta_1 + \ldots + a_{e-1}\,\eta_{e-1},\\
\eta\eta_1 &= b_0\eta_0 + b_1\eta_1 + \ldots + b_{e-1}\,\eta_{e-1},\\
&\vdots\\
\eta\eta_{e-1} &= l_0\eta_0 + l_1\eta_1 + \ldots + l_{e-1}\,\eta_{e-1}.
\end{aligned}$$

From these e linear equations $\eta_0, \eta_1, \ldots \eta_{e-1}$ may be eliminated and the result appears in the form

$$F(\eta) = \begin{vmatrix} (\eta - a_0), & -a_1, & -a_2, \ldots, & -a_{e-1} \\ -b_0, & (\eta - b_1), & -b_2, \ldots, & -b_{e-1} \\ \vdots & & & \\ -l_0, & -l_1, & -l_2, \ldots, & (\eta - l_{e-1}) \end{vmatrix} = 0.$$

Thus, for instance, in the example already considered $(p=13)$, if we take $\eta = \eta_0$ we have

$$\begin{aligned}
\eta\eta_0 - \eta_1 - 2\eta_2 \qquad\qquad &= 0\\
-\eta_0 + (\eta-1)\,\eta_1 \qquad - \eta_3 &= 0\\
3\eta_0 + 2\eta_1 + (\eta+3)\,\eta_2 + 2\eta_3 &= 0\\
-\eta_0 \qquad - \eta_2 + (\eta-1)\,\eta_3 &= 0:
\end{aligned}$$

whence

$$\begin{vmatrix} \eta, & -1, & -2, & 0 \\ -1, & \eta-1, & 0, & -1 \\ 3, & 2, & \eta+3, & 2 \\ -1, & 0, & -1, & \eta-1 \end{vmatrix} = 0,$$

which reduces to

$$\eta^4 + \eta^3 + 2\eta^2 - 4\eta + 3 = 0.$$

The reader who wishes for more numerical illustrations should consult Reuschle's *Tafeln Complexer Primzahlen* (Berlin, 1875).

179. Every root of $F(\eta)=0$ may be expressed as a rational integral function of any one assigned root η.

Suppose, for instance, we put $\eta=\eta_0$; then we can form the system of equations

$$\begin{aligned}
-1 &= \eta_0+\eta_1+\eta_2+\ldots+\eta_{e-1},\\
\eta_0 &= \eta_0,\\
\eta_0^2 &= a_0\eta_0+a_1\eta_1+a_2\eta_2+\ldots+a_{e-1}\,\eta_{e-1},\\
\eta_0^3 &= b_0\eta_0+b_1\eta_1+b_2\eta_2+\ldots+b_{e-1}\,\eta_{e-1},\\
&\vdots\\
\eta_0^{e-1} &= l_0\eta_0+l_1\eta_1+l_2\eta_2+\ldots+l_{e-1}\,\eta_{e-1},
\end{aligned}$$

and hence, if Δ is the determinant formed by the coefficients on the right-hand side, we have, for all values of k,

$$\Delta\,.\,\eta_k=A_0+A_1\eta_0+A_2\eta_0^2+\ldots+A_{e-1}\,\eta_0^{e-1},$$

where $A_0, A_1, \ldots A_{e-1}$ are integers. This proves the proposition, provided that Δ is not zero. But Δ cannot vanish, because if it did η_0 would satisfy the equation

$$A_0+A_1\eta_0+\ldots+A_{e-1}\,\eta_0^{e-1}=0,$$

which is impossible, since $F(\eta)$ is an irreducible function.

The method of this article affords another way of constructing the equation $F(\eta)=0$: namely by combining with the above system of equations the similar one

$$\eta_0^e=m_0\eta_0+m_1\eta_1+m_2\eta_2+\ldots+m_{e-1}\,\eta_{e-1},$$

and then eliminating $\eta_1, \eta_2, \ldots \eta_{e-1}$.

As an illustration, the reader may verify that for the trinomial periods $\eta_0, \eta_1, \eta_2, \eta_3$ associated with $p=13$,

$$\begin{aligned}
3\eta_1 &= -6+4\eta_0+3\eta_0^2+2\eta_0^3,\\
3\eta_2 &= 3-2\eta_0-\eta_0^3,\\
3\eta_3 &= -5\eta_0-3\eta_0^2-\eta_0^3.
\end{aligned}$$

180. Each of the f roots of $X=0$, the aggregate of which makes up any one of the f-nomial periods, satisfies an equation of the fth degree, the coefficients of which are linear functions of the periods with integral coefficients.

It has already been observed (Art. 175) that the effect of changing r into r^{g^e} is to produce a cyclical permutation of the roots which make up a period: hence all symmetric functions of these roots remain unaltered, and may therefore be expressed as linear functions of the periods. This proves the proposition.

Thus, in the case already chosen for illustration, the roots r, r^3, r^9, of which the sum is η_0, satisfy the equation

$$x^3 - \eta_0 x^2 + \eta_2 x - 1 = 0\,;$$

and in the same way the equations

$$x^3 - \eta_1 x^2 + \eta_3 x - 1 = 0,$$
$$x^3 - \eta_2 x^2 + \eta_0 x - 1 = 0,$$
$$x^3 - \eta_3 x^2 + \eta_1 x - 1 = 0,$$

are satisfied by (r^2, r^5, r^6), (r^4, r^{10}, r^{12}), and (r^7, r^8, r^{11}) respectively.

Remembering that η_0 may be any root of

$$F(\eta) = \eta^4 + \eta^3 + 2\eta^2 - 4\eta + 3 = 0,$$

and that η_1, η_2, η_3 can be expressed as rational functions of η_0, we see that by the 'adjunction' of the single irrationality η_0, which is defined by the equation $F(\eta) = 0$, the polynomial X_{13} may be resolved into the product of four polynomials each of the third degree; so that the solution of $X_{13} = 0$, which is of the twelfth degree, is reduced to that of one quartic and three cubic equations.

But in the case considered the reduction may be carried one stage further. There are two periods of six terms,

$$\zeta_1 = \eta_0 + \eta_2,$$
$$\zeta_2 = \eta_1 + \eta_3,$$

and it is easily verified that

$$\zeta_1 + \zeta_2 = -1,$$
$$\zeta_1 \zeta_2 = -3:$$

so that ζ_1, ζ_2 are the roots of

$$z^2 + z - 3 = 0.$$

Moreover $\eta_0 \eta_2 = \eta_1 + \eta_3 + 3 = \zeta_2 + 3$: hence η_0, η_2 are the roots of $y^2 - \zeta_1 y + (\zeta_2 + 3) = 0$, and in the same way η_1, η_3 are the roots of $y^2 - \zeta_2 y + (\zeta_1 + 3) = 0$. Hence the solution of

$$\eta^4 + \eta^3 + 2\eta^2 - 4\eta - 3 = 0$$

is made to depend upon the system of auxiliary quadratics

$$z^2 + \ z - 3 \ = 0,$$
$$y^2 - \zeta_1 y + (\zeta_2 + 3) = 0,$$
$$y^2 - \zeta_2 y + (\zeta_1 + 3) = 0.$$

The algebraical solution of $X_{13}=0$ may therefore be stated in the following form:—

Let ζ be any root of $\quad z^2+z-3=0,$
η any root of $\quad y^2-\zeta y+(2-\zeta)=0,$
ξ any root of $\quad x^3-\eta x^2+(\zeta-\eta)\,x-1=0;$
then $x=\xi$ is a solution of $X_{13}=0$.

181. In the general case, whenever e is a composite number, say $e'f'$, the expressions

$$\begin{aligned}\zeta_0 &= \eta_0 + \eta_{e'} + \eta_{2e'} + \ldots + \eta_{(f'-1)e'},\\ \zeta_1 &= \eta_1 + \eta_{e'+1} + \eta_{2e'+1} + \ldots + \eta_{(f'-1)e'+1},\\ &\vdots\\ \zeta_{e'-1} &= \eta_{e'-1} + \eta_{2e'-1} + \eta_{3e'-1} + \ldots + \eta_{e-1},\end{aligned}$$

are periods, and will satisfy an equation $F_1(\zeta)=0$ of degree e' with integral coefficients; and by the adjunction of a root of this equation, the polynomial $F(\eta)$ may be resolved into the product of e' polynomials, the coefficients of which are integral functions of ζ.

In the same way, if f is a composite number, say e_1f_1, any period η_k may be expressed as the sum of e_1 periods, each of f_1 terms; and the f_1-nomial periods of each such group are the roots of an equation of degree e_1 whose coefficients are rational functions of the η's, or, which is the same thing, of any one of them.

Proceeding in this way we see that the solution of $X_p=0$ may be obtained from a system of auxiliary equations, the degrees of which are the prime factors of $(p-1)$; the number of the equations being equal to the number of factors.

The system of equations will depend upon the way in which the roots of $X=0$ are distributed into successive groups of periods. Practically, it is best to keep conjugate roots r^h, r^{-h} together in the same period until the last stage of all, because then the roots of the auxiliary equations will all be real, except in the case of the last, which will be a quadratic with complex roots. Thus, for instance, when $p=13$, we may begin with the three periods of four terms, and form the auxiliary system

$$\begin{aligned}z^3+z^2-4z+1&=0,\\ y^2-\zeta y+(\zeta^2+\zeta-3)&=0,\\ x^2-\eta x+1&=0,\end{aligned}$$

where ζ is any root of the first equation, and η is any root of the second.

The solutions of $X_{17}=0$ and $X_{19}=0$ are given explicitly in Arts. 353, 354 of the *Disquisitiones Arithmeticæ*: the reader may also consult Richelot, *De resolutione algebraica æquationis* $X^{257}=1$, etc. (Crelle ix. (1832), p. 1), and Cayley, *Note sur la solution de l'équation* $x^{257}-1=0$ (ibid. xli. (1851), p. 81).

It is now well known that there is no general formula for expressing the root of an equation as an algebraic function of the coefficients, when the degree of the equation exceeds 4. This was to some extent anticipated by Gauss (*D. A.* Art. 359, with the reference there given), but was first proved by Abel. Now the degrees of the auxiliary equations, upon which the solution of $X_p=0$ has been made to depend, are the prime factors of $(p-1)$, some of which may, and in general will, exceed 3. Hence Gauss's theory of the periods gives us no assurance that the roots of $X_p=0$ may be obtained in the form of purely algebraical irrationalities. That this is in fact the case was discovered by Gauss, whose method was afterwards simplified by Jacobi; but since the interest of the problem is mainly algebraical, and its solution immediately follows from the principles laid down in Abel's memoir on equations which are solvable by radicals, we prefer to pass on to applications which are more distinctly arithmetical in character[1].

182. If q is a prime of the form $\lambda p+1$, where p, as before, is an odd prime, the congruence $x^p-1\equiv 0 \pmod q$ has all its roots real, and the same will therefore be the case with $X_p=0 \pmod q$. All the algebraical theory of the equation $X_p=0$ may be applied *mutatis mutandis* to the congruence $X_p\equiv 0 \pmod q$: thus we may arrange the roots of the congruence into periods, and reduce the solution of $X_p\equiv 0$ to that of a set of auxiliary congruences, etc. etc. For example, if $p=13$, $q=53$, we may take as a system of auxiliary congruences for the solution of $X_{13}\equiv 0 \pmod{53}$

$$\left.\begin{aligned} z^2+z-3&\equiv 0\\ y^2-\zeta y+(2-\zeta)&\equiv 0\\ x^3-\eta x^2+(\zeta-\eta)x-1&\equiv 0\end{aligned}\right\}\quad \pmod{53}.$$

[1] For the explicit solution of $X_p=0$ the reader should consult Gauss, *Disq. Arith.* Arts. 359—60, and the posthumous paper *Disquisitionum circa æquationes puras ulterior evolutio* (Werke ii. 243); Jacobi, *Ueber die Kreistheilung und ihre Anwendung auf die Zahlentheorie* (Berl. Monatsb., Oct. 1837, p. 127, or Crelle xxx. p. 166); Abel, *Mémoire sur une classe particulière d'équations résolubles algébriquement* (Crelle iv. (1829), p. 131). See also Bachmann's *Kreistheilung*, 8te Vorlesung, where other references will be found.

The first may be written $(z-7)(z+8)\equiv 0$; if we take $\zeta\equiv 7$, the second congruence becomes

$$y^2-7y-5\equiv 0,$$

or

$$(y+21)(y-28)\equiv 0.$$

Putting $\eta\equiv -21$, we have

$$x^3+21x^2+28x-1\equiv 0,$$

whence $x\equiv -6,\ 12,\ 14$. All the roots of $X_{13}\equiv 0$ are given by $x\equiv(-6)^k$, where $k=1,\ 2,\ldots 12$.

It may be specially noticed that corresponding to the equation $F(\eta)=0$, satisfied by the f-nomial periods (Art. 177), we have a congruence $F(\eta)\equiv 0 \pmod q$ all the roots of which are real, and connected by congruential relations precisely similar to those which are satisfied by the algebraical periods. Thus, for instance, when $p=13$, we have a period-equation (Art. 178)

$$\eta^4+\eta^3+2\eta^2-4\eta+3=0;$$

the roots of the corresponding congruence, mod 53, are

$$\eta\equiv 14,\ -21,\ -22,\ -25.$$

If we put $\eta_0\equiv 14$, then in order that the relations connecting the roots may be the same as for the corresponding equations, we *must* write

$$\eta_1\equiv -25,\ \eta_2\equiv -22,\ \eta_3\equiv -21;$$

and so, in general, when any root of the congruence has been chosen to correspond to a particular period, say η_0, the relation of the other roots to the remaining periods is determined (cf. Art. 174).

The results of this article were evidently familiar to Gauss, although he did not publish them; see the paper entitled *Solutio congruentiæ* $x^m-1\equiv 0$, which is printed in the second volume of his works (p. 199). It will be seen, later on, what important consequences have been deduced from them by Cauchy, Kummer, and others.

183. For every odd prime p there will be two periods, each containing $\frac{1}{2}(p-1)$ terms; denoting them by A and B, we may write, in our previous notation,

$$A=r\ +r^{g^2}+r^{g^4}+\ldots+r^{g^{p-3}},$$

$$B=r^{g}+r^{g^3}+r^{g^5}+\ldots+r^{g^{p-2}}.$$

Since 1, $g^2, g^4, \dots g^{p-3}$ are all incongruent with respect to p, we have $A = \Sigma r^\alpha$, where the summation extends to all the positive quadratic residues of p which are less than p; and in the same way $B = \Sigma r^\beta$, where β denotes any one of the quadratic non-residues of p which are positive and less than p.

In order to find the quadratic equation of which A and B are the roots, we may calculate the values of $A+B$ and AB. We have at once $A+B=-1$, but the determination of AB is less easy. We know (Art. 177), that its value is a real integer; moreover it may be written in the form

$$AB = \Sigma r^{\alpha+\beta},$$

where the sum on the right contains $\frac{1}{4}(p-1)^2$ terms. The term $r^{\alpha+\beta}$ reduces to 1 if

$$\alpha+\beta=p;$$

this gives $-\beta \equiv \alpha \pmod{p}$, which can only happen if -1 is a non-residue of p, that is to say, if $p \equiv 3 \pmod 4$. Conversely, if this is the case, for every term r^α which occurs in A there is a corresponding term $r^{p-\alpha}$ in B, and when we multiply A and B together, we obtain $\frac{1}{2}(p-1)$ terms each equal to unity. The remaining terms of the product, $\frac{1}{4}(p-1)^2 - \frac{1}{2}(p-1)$ in number, must reduce to $r + r^2 + \dots + r^{p-1}$, that is -1, taken

$$\frac{\frac{1}{4}(p-1)^2 - \frac{1}{2}(p-1)}{p-1} = \frac{1}{4}(p-3)$$

times; hence $AB = \frac{1}{2}(p-1) - \frac{1}{4}(p-3) = \frac{1}{4}(p+1)$, and the equation satisfied by A and B is

$$\eta^2 + \eta + \tfrac{1}{4}(p+1) = 0.$$

On the other hand, if $p \equiv 1 \pmod 4$, it is impossible that $\alpha+\beta=p$, so that in this case

$$AB = -1 \times \frac{\frac{1}{4}(p-1)^2}{(p-1)} = -\tfrac{1}{4}(p-1),$$

and the quadratic in η is

$$\eta^2 + \eta - \tfrac{1}{4}(p-1) = 0.$$

Both cases are included in the formula

$$\eta^2 + \eta + \frac{1-(-1)^{\frac{1}{2}(p-1)}p}{4} = 0.$$

184. If we solve the quadratic we obtain

$$\eta = \frac{-1 \pm i^{\frac{1}{2}(p-1)}\sqrt{p}}{2};$$

now when p and r have been chosen the value of A is perfectly determinate, and the question arises how the ambiguity is to be taken when r and p are assigned. We observe that if r is changed into r^m, where m is prime to p, A and B remain unaltered, or are interchanged, according as m is or is not a quadratic residue of p. Hence it is sufficient to find the value of A for any one value of r; we shall suppose that $r = e^{2\pi i/p}$. This being so, the value of A may be written

$$A = e^{2\pi i/p} + e^{8\pi i/p} + e^{18\pi i/p} + \ldots + e^{\frac{1}{2}(p-1)^2\pi i/p}$$

$$= \sum_{s=1}^{s=\frac{1}{2}(p-1)} e^{2s^2\pi i/p}.$$

Instead of this we shall consider the slightly more general expression

$$S = \sum_{s=0}^{s=n-1} e^{2s^2\pi i/n},$$

where n is any positive real integer, and the sum consists of n terms. The determination of the value of S has lately been effected by Kronecker in a remarkably simple and elegant manner with the help of Cauchy's theory of complex integration (Crelle cv. (1889), p. 267); his investigation will therefore be given here before discussing the less direct, although more arithmetical, methods of Gauss and Dirichlet.

Consider the expression

$$\phi(z) = \frac{e^{2\pi i z^2/n}}{1 - e^{2\pi i z}};$$

this is a one-valued function of the complex variable z which is finite and continuous for all finite values of z, except when z is a real integer. Putting $z = h$, a real integer, we have

$$\operatorname*{Lt.}_{z=h} (z-h)\,\phi(z) = -\frac{1}{2\pi i}\, e^{2\pi i h^2/n},$$

so that $z = h$ is a simple pole of $\phi(z)$.

Now by a well-known theorem, due to Cauchy, the integral $\int \phi(z)\,dz$, taken in the positive direction round any closed contour C which encloses a certain number of poles of $\phi(z)$, is equal to the sum of the values of the same integral taken in the positive direction round closed contours each surrounding one of the poles enclosed by C.

To apply this to the present case, we choose for the contour C that which is represented in Fig. 6. It consists of a rectangle with two semicircular notches cut out of it: the vertices of the rectangle are $\pm iy_1$, $\frac{1}{2}n \pm iy_1$, and the terminal points of the semicircles are at $\pm iy_0$, $\frac{1}{2}n \pm iy_0$ respectively. We shall eventually make $y_1 = +\infty$ and y_0 infinitesimal: and it will be supposed in the first instance that $y_0 < \frac{1}{2}$; thus if n is odd, the poles within C are $1, 2, 3 \ldots \frac{1}{2}(n-1)$, and if n is even they are $1, 2, 3, \ldots (\frac{1}{2}n - 1)$.

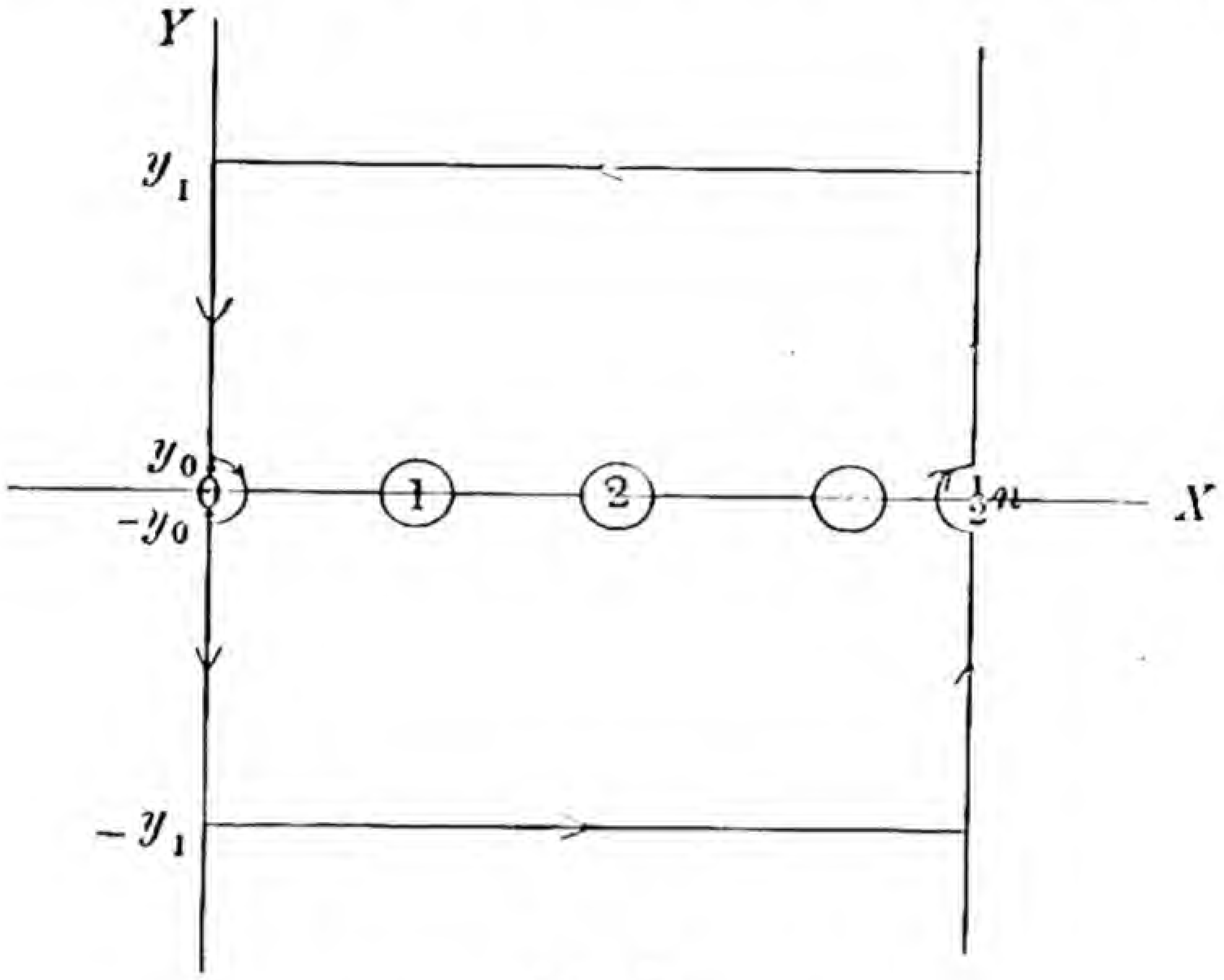

Fig. 6.

First suppose that n is odd. The value of $\int\phi(z)\,dz$ taken round an infinitesimal circle surrounding the pole $z = s$ is

$$-\frac{1}{2\pi i} e^{2\pi i s^2/n} \,.\, 2\pi i = -e^{2\pi i s^2/n}.$$

Next consider the integration over C. The semicircle at the origin gives ultimately, when y_0 is infinitesimal,

$$-\frac{1}{2\pi i}\int_{\frac{\pi}{2}}^{-\frac{\pi}{2}} i\,d\theta = \tfrac{1}{2};$$

the other semicircle gives nothing, since $\frac{1}{2}n$ is not a pole.

The remaining part of the integration gives

$$\left.\begin{array}{l}\displaystyle\int_{-y_0}^{-y_1} i\phi(it)\,dt + \int_0^{\frac{1}{2}n} \phi(-iy_1 + t)\,dt + \int_{-y_1}^{-y_0} i\phi(\tfrac{1}{2}n + it)\,dt \\ \displaystyle\quad + \int_{y_0}^{y_1} i\phi(\tfrac{1}{2}n + it)\,dt + \int_{\frac{1}{2}n}^{0} \phi(iy_1 + t)\,dt + \int_{y_1}^{y_0} i\phi(it)\,dt\end{array}\right\} \text{(A)},$$

where t is a real variable.

Now it is easily seen that the second and fifth of these integrals ultimately vanish when $y_1 = +\infty$, because

$$\phi(-iy_1 + t) = \frac{e^{2\pi i(-iy_1+t)^2/n}}{1 - e^{2\pi i(-iy_1+t)}}$$
$$= e^{-2\pi y_1(1-2t/n)} \,.\, \psi(t),$$

where $\psi(t)$ does not become infinite, and $y_1(1 - 2t/n)$ is not negative; while

$$\phi(iy_1 + t) = e^{-4\pi t y_1/n} \,.\, \chi(t),$$

where $\chi(t)$ does not become infinite. In each case the exponential factor causes the integral to vanish.

The first integral in (A) may be written

$$-i\int_{y_0}^{y_1} \phi(-it)\,dt\,;$$

hence the sum of the first and last

$$= -i\int_{y_0}^{y_1} \{\phi(it) + \phi(-it)\}\,dt,$$
$$= -i\int_{y_0}^{y_1} e^{-2\pi i t^2/n} \,.\, dt$$

on reduction.

With regard to the other two integrals, we observe that

$$\phi(\tfrac{1}{2}n + it) = \frac{i^n e^{-2\pi t} \,.\, e^{-2\pi i t^2/n}}{1 - (-1)^n e^{-2\pi t}},$$
$$\phi(\tfrac{1}{2}n - it) = \frac{i^n e^{2\pi t} \,.\, e^{-2\pi i t^2/n}}{1 - (-1)^n e^{2\pi t}};$$

whence the sum of the remaining integrals

$$= i\int_{y_0}^{y_1} \{\phi(\tfrac{1}{2}n + it) + \phi(\tfrac{1}{2}n - it)\}\,dt,$$
$$= -(-1)^n i^{n+1} \int_{y_0}^{y_1} e^{-2\pi i t^2/n}\,dt = -i^{3n+1}\int_{y_0}^{y_1} e^{-2\pi i t^2/n} \,.\, dt.$$

If we make y_0 infinitesimal and y_1 infinite, we have ultimately

$$\int_{y_0}^{y_1} e^{-2\pi i t^2/n}\,dt = \sqrt{n}\int_{y_0/\sqrt{n}}^{y_1/\sqrt{n}} e^{-2\pi i u^2}\,du$$
$$= \sqrt{n}\int_0^{\infty} e^{-2\pi i u^2}\,du$$
$$= A\sqrt{n}$$

where $\sqrt{n}$ is taken positively, and A is a constant which is independent of n. Hence finally, n being odd,

$$\tfrac{1}{2} - (i + i^{3n+1})\,A\sqrt{n} = -\sum_{s=1}^{s=\frac{1}{2}(n-1)} e^{2\pi i s^2/n},$$

or, multiplying by 2 and transposing,

$$S=2A\sqrt{n}\,(i+i^{3n+1}).$$

To determine A, put $n=3$: then $S=i\sqrt{3}$, so that

$$i=2A\,(i-1)\,;$$

therefore $$A=\frac{1}{2+2i},$$

and $$S=\frac{i\,(1+i^{3n})}{1+i}\sqrt{n}.$$

This may also be written

$$S=\frac{i+i^{1-n}}{1+i}\sqrt{n},$$

which is Kronecker's form of the result. It must be carefully remembered that $\sqrt{n}$ is the positive square root of n.

The same formula applies when n is even; the only difference in the work is that $\frac{1}{2}n$ is now a pole, and the semicircle at $\frac{1}{2}n$ ultimately contributes $\frac{1}{2}$ instead of zero to the integration round C.

The results may be tabulated according to the residue of n to modulus 4. Thus if

$$\begin{array}{ll} n\equiv 0 \pmod{4}, & S=(1+i)\sqrt{n}, \\ \quad\equiv 1 & \quad=\sqrt{n} \\ \quad\equiv 2 & \quad=0 \\ \quad\equiv 3 & \quad=i\sqrt{n}. \end{array}$$

Suppose, now, that n is an odd prime p; then the expression denoted by A in the beginning of this article is equal to $\frac{1}{2}(S-1)$, that is, to

$$\frac{-1+\sqrt{p}}{2} \text{ or } \frac{-1+i\sqrt{p}}{2},$$

according as $p\equiv 1$ or $3 \pmod{4}$.

185. Dirichlet's method is somewhat analogous to the preceding, but avoids the use of the complex variable. It depends upon the lemma that if $f(x)$ is a function of x which is finite and continuous so long as $0 \ngtr x \ngtr \pi$,

$$\sum_{-\infty}^{+\infty}\int_0^\pi f(x)\,.\cos sx\,dx=\pi f(0),$$

where the summation applies to all integral values of s.

Observing that, if r is a positive integer,

$$\int_{2r\pi}^{(2r+1)\pi} f(x)\,.\cos sx\,.\,dx = \int_0^\pi f(2r\pi + x)\cos sx\,dx,$$

$$\int_{(2r+1)\pi}^{(2r+2)\pi} f(x)\,.\cos sx\,.\,dx = \int_0^\pi f(\overline{2r+2}\,.\,\pi - x)\cos sx\,dx,$$

we infer that if h is a positive integer, and $f(x)$ satisfies the same conditions as before so long as $0 \not> x \not> 2h\pi$,

$$\sum_{-\infty}^{+\infty}\int_0^{2h\pi} f(x)\cos sx\,dx = \sum_{-\infty}^{+\infty}\left\{\int_0^\pi + \int_\pi^{2\pi} + \ldots + \int_{(2h-1)\pi}^{2h\pi}\right\} f(x)\cos sx\,dx$$

$$= \sum_{-\infty}^{+\infty}\int_0^\pi \{f(x)+f(2\pi-x)+f(2\pi+x)+\ldots f(2h\pi-x)\}\cos sx\,dx$$

$$= \pi\{f(0)+2f(2\pi)+2f(4\pi)+\ldots+2f(\overline{2h-2}\,.\,\pi)+f(2\pi)\}.$$

Consider now the integrals

$$u = \int_{-\infty}^{+\infty}\cos x^2\,dx = 2\int_0^\infty \frac{\cos y}{\sqrt{y}}\,dy,$$

$$v = \int_{-\infty}^{+\infty}\sin x^2\,dx = 2\int_0^\infty \frac{\sin y}{\sqrt{y}}\,dy;$$

it is easily seen that these are finite and determinate, in whatever way the upper limit of integration is supposed to become infinite. Writing αx^2 for x^2, where α is finite and positive, we find

$$\int_{-\infty}^{+\infty}\cos \alpha x^2\,.\,dx = u/\sqrt{\alpha}, \quad \int_{-\infty}^{+\infty}\sin \alpha x^2\,.\,dx = v/\sqrt{\alpha},$$

$\sqrt{\alpha}$ being taken positively: and hence, if

$$\Delta = \int_{-\infty}^{+\infty}\cos(\delta + x^2)\,dx = u\cos\delta - v\sin\delta,$$

where δ is any finite quantity, we have

$$\int_{-\infty}^{+\infty}\cos(\delta + \alpha x^2)\,dx = \frac{\Delta}{\sqrt{\alpha}}.$$

Now let β be a finite positive quantity: then the integral last written may be replaced by

$$\sum_{-\infty}^{+\infty}\int_{s\beta}^{(s+1)\beta}\cos(\delta + \alpha x^2)\,dx$$

where the summation extends to all integral values of s.

But $\displaystyle\int_{s\beta}^{(s+1)\beta}\cos(\delta + \alpha x^2)\,dx = \int_0^\beta \cos\{\delta + \alpha(s\beta + x)^2\}\,dx,$

and if we put $\beta = 4m\pi$, $\alpha = 1/8m\pi$, where m is a positive integer, this reduces to

$$\int_0^{4m\pi} \cos\left(\delta + sx + \frac{x^2}{8m\pi}\right) dx$$

$$= \int_0^{4m\pi} \cos\left(\delta + \frac{x^2}{8m\pi}\right) \cos sx\, dx - \int_0^{4m\pi} \sin\left(\delta + \frac{x^2}{8m\pi}\right) \sin sx\, dx.$$

Since the second integral on the right hand is an odd function of x, and we may suppose the values of s arranged in the order $s = 0, \pm 1, \pm 2, \ldots \pm h$ where h is an indefinitely large integer, we have finally

$$\frac{\Delta}{\sqrt{\alpha}} = \Delta\sqrt{8m\pi} = \sum_{-\infty}^{+\infty} \int_0^{4m\pi} \cos\left(\delta + \frac{x^2}{8m\pi}\right) \cos sx\, dx.$$

Writing, for the moment,

$$\cos\left(\delta + \frac{x^2}{8m\pi}\right) = f(x),$$

the application of the previous lemma gives

$$\Delta\sqrt{8m\pi} = \pi\{f(0) + 2f(2\pi) + 2f(4\pi) + \ldots + 2f(\overline{4m-2}\,.\,\pi) + f(4m\pi)\}.$$

Now, if s is any integer, $f(4m\pi + 2s\pi) = f(2s\pi)$: hence the expression on the right may be replaced by

$$\pi\{f(0) + f(2\pi) + \ldots + f(4m\pi) + f(\overline{4m+2}\,.\,\pi) + \ldots + f(\overline{8m-2}\,.\,\pi)\}$$

$$= \pi \sum_0^{4m-1} f(2s\pi);$$

therefore

$$\Delta\sqrt{8m\pi} = \pi \sum_0^{4m-1} \cos\left(\delta + \frac{s^2\pi}{2m}\right) = \pi\left\{\cos\delta \sum_0^{4m-1} \cos\frac{s^2\pi}{2m} - \sin\delta \sum_0^{4m-1} \sin\frac{s^2\pi}{2m}\right\}.$$

Since $\Delta = u\cos\delta - v\sin\delta$, and the formula is true for all values of δ, it follows that

$$\sum_0^{4m-1} \cos\frac{s^2\pi}{2m} = u\sqrt{8m/\pi}, \qquad \sum_0^{4m-1} \sin\frac{s^2\pi}{2m} = v\sqrt{8m/\pi}.$$

To determine u and v, which are evidently independent of m, we put $m = 1$, which gives $u = v = \sqrt{\tfrac{1}{2}\pi}$; and hence finally

$$\sum_0^{4m-1} \cos\frac{s^2\pi}{2m} = \sum_0^{4m-1} \sin\frac{s^2\pi}{2m} = 2\sqrt{m}.$$

Following Dirichlet, we shall write

$$\sum_0^{n-1} e^{2hs^2\pi i/n} = \phi(h, n),$$

where n is a positive integer, and h is also integral but not necessarily positive. Thus the result which we have just obtained may be expressed by the formula

$$\phi(1,\ 4m) = 2(1+i)\sqrt{m},$$

or, which is the same thing,

$$\phi(1,\ n) = (1+i)\sqrt{n}, \text{ if } n \equiv 0 \pmod{4}.$$

186. It immediately follows from the definition that if

$$h' \equiv h \pmod{n},\ \phi(h',\ n) = \phi(h,\ n).$$

Moreover, if a is any integer prime to n,

$$\phi(ha^2,\ n) = \phi(h,\ n):$$

because by definition $\phi(ha^2,\ n) = \sum\limits_0^{n-1} e^{2h(as)^2\pi i/n}$, and when s assumes the values $0,\ 1,\ 2 \ldots (n-1)$, the least positive residues of as to modulus n consist of the same numbers in a different order.

Another theorem which we shall require is the following:—

If the positive integers m, n are prime to each other, then

$$\phi(hm,\ n) \,.\, \phi(hn,\ m) = \phi(h,\ mn).$$

To prove this, we observe that, by definition,

$$\phi(hm,\ n) \,.\, \phi(hn,\ m) = \sum_{s,\ t} e^{2h\pi i\left(\frac{ms^2}{n} + \frac{nt^2}{m}\right)}; \qquad \begin{pmatrix} s = 0,\ 1,\ 2,\ \ldots\ n-1 \\ t = 0,\ 1,\ 2,\ \ldots\ m-1 \end{pmatrix}$$

now

$$\frac{ms^2}{n} + \frac{nt^2}{m} = \frac{(ms+nt)^2}{mn} - 2st,$$

therefore

$$\phi(hm,\ n) \,.\, \phi(hn,\ m) = \sum_{s,\ t} e^{2h\pi i(ms+nt)^2/mn}.$$

But the expression $ms + nt$ assumes mn values altogether, and it is easily proved that these are all incongruent (mod mn), because if

$$ms' + nt' \equiv ms + nt \pmod{mn},$$

we infer that $ms' \equiv ms \pmod{n}$ and $nt' \equiv nt \pmod{m}$, whence $s' \equiv s \pmod{n}$ and $t' \equiv t \pmod{m}$, whereas in the present case all the values of s are incongruent (mod n) and all the values of t are incongruent (mod m).

Hence the integers $ms + nt$ form a complete system of residues to modulus mn, and therefore

$$\sum_{s,\ t} e^{2h\pi i(ms+nt)^2/mn} = \sum_0^{mn-1} e^{2hs^2\pi i/mn} = \phi(h,\ mn),$$

and the theorem is proved.

187. Suppose, now, that n is an odd number; then, putting $m=4$, $h=1$, we obtain

$$\phi(4, n)\,\phi(n, 4) = \phi(1, 4n).$$

As already proved, $\phi(1, 4n) = 2(1+i)\sqrt{n}$, and by definition

$$\begin{aligned}\phi(n, 4) &= 1 + e^{2n\pi i/4} + e^{8n\pi i/4} + e^{18n\pi i/4}\\ &= 2(1+i^n);\end{aligned}$$

moreover, by putting $h=1$, $a=2$ in the formula

$$\phi(ha^2, n) = \phi(h, n),$$

we find

$$\phi(4, n) = \phi(1, n);$$

hence

$$2(1+i^n)\,\phi(1, n) = 2(1+i)\sqrt{n},$$

or

$$\begin{aligned}\phi(1, n) &= \frac{1+i}{1+i^n}\sqrt{n}\\ &= \sqrt{n} \text{ or } i\sqrt{n},\end{aligned}$$

according as $n \equiv 1$ or $3 \pmod 4$.

Finally let $n \equiv 2 \pmod 4$; then, since 2 is prime to $\tfrac{1}{2}n$, we have

$$\phi(2, \tfrac{1}{2}n)\,.\,\phi(\tfrac{1}{2}n, 2) = \phi(1, n),$$

but $\phi(\tfrac{1}{2}n, 2) = \phi(1, 2) = 0$; therefore $\phi(1, n) = 0$. The value of $\phi(1, n)$ has now been determined for all integral values of n: the results are, of course, in agreement with those of Art. 184, because $\phi(1, n)$ is the expression there denoted by S.

188. We will now give some account of Gauss's demonstration, which, as already remarked, has the advantage of not requiring the aid of any transcendental analysis except the elementary theory of the circular functions.

Consider the expression

$$(m, \mu) = \frac{(1-x^m)(1-x^{m-1})(1-x^{m-2})\ldots(1-x^{m-\mu+1})}{(1-x)(1-x^2)(1-x^3)\ldots(1-x^\mu)},$$

where m, μ are positive integers. If $m < \mu$, the numerator involves the factor $1-x^0$, and therefore $(m, \mu) = 0$; we proceed to prove that if $m \nless \mu$, (m, μ) is a rational integral function of x.

It is obvious, in the first place, that

$$(m, m-\mu) = (m, \mu),$$

if $m \nless \mu$; and also that $(\mu, \mu) = 1$.

Again, since

$$1 - x^m = (1 - x^{m-\mu-1}) + x^{m-\mu-1}(1 - x^{\mu+1}),$$

it follows that $(m, \mu+1)$

$$= \frac{\{(1-x^{m-\mu-1}) + x^{m-\mu-1}(1-x^{\mu+1})\}(1-x^{m-1})\ldots(1-x^{m-\mu})}{(1-x)(1-x^2)\ldots(1-x^{\mu+1})}$$

$$= (m-1, \mu+1) + x^{m-\mu-1}(m-1, \mu)$$

$$= (m-2, \mu+1) + x^{m-\mu-2}(m-2, \mu) + x^{m-\mu-1}(m-1, \mu)$$

$$= \ldots\ldots\ldots$$

$$= (\mu+1, \mu+1) + x(\mu+1, \mu) + x^2(\mu+2, \mu) + \ldots + x^{m-\mu-1}(m-1, \mu)$$

$$= 1 + x(\mu+1, \mu) + x^2(\mu+2, \mu) + \ldots + x^{m-\mu-1}(m-1, \mu),$$

supposing that $m \nless \mu+2$.

Hence if, for any fixed value of μ, the expression (m, μ) is a rational integral function of x for all positive integral values of m, the same will be true of $(m, \mu+1)$. But $(m, 1) = (1-x^m)/(1-x)$, which is a rational integral function; therefore the theorem is true for $(m, 2)$, and hence successively for $(m, 3)$, $(m, 4)$, and so on. This proves the proposition.

189. Now let us write

$$f(x, m) = 1 - \frac{1-x^m}{1-x} + \frac{(1-x^m)(1-x^{m-1})}{(1-x)(1-x^2)} - \ldots$$
$$= 1 - (m, 1) + (m, 2) - (m, 3) + \ldots.$$

This contains $(m+1)$ terms, the last being $(-1)^m$, and since, by the proposition just proved, each term is a rational integral function of x, $f(x, m)$ is also a polynomial in x.

If m is odd, $f(x, m) = 0$ identically, because the first term cancels out with the last, the second with the last but one, and so on.

Next, suppose m is even. We have identically

$$\begin{aligned} 1 &= 1 \\ -(m, 1) &= -(m-1, 1) - x^{m-1} \\ +(m, 2) &= +(m-1, 2) + x^{m-2}(m-1, 1) \\ -(m, 3) &= -(m-1, 3) - x^{m-3}(m-1, 2), \end{aligned}$$

and so on; whence, by addition

$$\begin{aligned} f(x,m) &= (1-x^{m-1}) - (1-x^{m-2})(m-1, 1) + (1-x^{m-3})(m-1, 2) - \ldots \\ &= (1-x^{m-1})\{1-(m-2, 1) + (m-2, 2) - \ldots \text{ to } (m-1) \text{ terms}\} \\ &= (1-x^{m-1}) f(x, m-2) \\ &= (1-x^{m-1})(1-x^{m-3}) f(x, m-4) \\ &= (1-x^{m-1})(1-x^{m-3})(1-x^{m-5})\ldots(1-x) f(x, 0) \\ &= (1-x)(1-x^3)(1-x^5)\ldots(1-x^{m-1}). \end{aligned}$$

190. Hitherto x has been any quantity whatever: we will now suppose that $x = e^{2\pi i/n}$, where n is an odd positive integer, and we will write m for $(n-1)$. This being so, we have

$$\frac{1-x^m}{1-x} = \frac{1-x^{-1}}{1-x} = -x^{-1},$$

$$\frac{1-x^{m-1}}{1-x^2} = \frac{1-x^{-2}}{1-x^2} = -x^{-2},$$

$$\dots\dots\dots\dots\dots\dots\dots\dots\dots$$

$$\frac{1-x^{m-\mu+1}}{1-x^\mu} = \frac{1-x^{-\mu}}{1-x^\mu} = -x^{-\mu};$$

hence

$$(m, \mu) = (-1)^\mu x^{-\frac{1}{2}\mu(\mu+1)},$$

and the identity

$$f(x, m) = (1-x)(1-x^3)(1-x^5)\dots(1-x^{m-1})$$

becomes

$$1 + x^{-1} + x^{-3} + \dots + x^{-\frac{1}{2}\mu(\mu+1)} + \dots + x^{-\frac{1}{2}n(n-1)}$$
$$= (1-x)(1-x^3)(1-x^5)\dots(1-x^{n-2}).$$

Since x^{-2}, like x, is a primitive root of $x^n - 1 = 0$, we may change x into x^{-2}, and thus obtain

$$1 + x^2 + x^6 + \dots + x^{\mu(\mu+1)} + \dots + x^{n(n-1)}$$
$$= (1-x^{-2})(1-x^{-6})\dots(1-x^{-2n+4}).$$

Multiply both sides by

$$x \,.\, x^3 \,.\, x^5 \dots x^{n-2} = x^{\frac{1}{4}(n-1)^2};$$

then on the right hand we have

$$(x - x^{-1})(x^3 - x^{-3})\dots(x^{n-2} - x^{-n+2}),$$

while, if we observe that

$$\tfrac{1}{4}(n-1)^2 + \mu(\mu+1) = \tfrac{1}{4}\{n^2 - 2n + (2\mu+1)^2\}$$
$$\equiv \tfrac{1}{4}(n - 2\mu - 1)^2 \pmod{n},$$

the expression on the left becomes

$$x^{\frac{1}{4}(n-1)^2} + x^{\frac{1}{4}(n-3)^2} + x^{\frac{1}{4}(n-5)^2} + \dots + x^{\frac{1}{4}(n+3)^2} + x^{\frac{1}{4}(n+1)^2}.$$

Rearranging this, we have finally

$$S = 1 + x + x^4 + \dots + x^{(n-1)^2} = (x - x^{-1})(x^3 - x^{-3})\dots(x^{n-2} - x^{-n+2}).$$

Now

$$x - x^{-1} = x^{-n+1} - x^{n-1},$$
$$x^3 - x^{-3} = x^{-n+3} - x^{n-3},$$

and so on: therefore

$$S^2 = (-1)^{\frac{1}{2}(n-1)} \,.\, (x - x^{-1})(x^2 - x^{-2})(x^3 - x^{-3})\dots(x^{n-1} - x^{-n+1})$$
$$= (-1)^{\frac{1}{2}(n-1)} \,.\, x^{\frac{1}{2}n(n+1)} \,.\, (1 - x^{-2})(1 - x^{-4})\dots(1 - x^{-2n+2})$$
$$= (-1)^{\frac{1}{2}(n-1)} n,$$

because $x^{\frac{1}{2}n(n+1)} = 1$, and $x^{-2}, x^{-4}, \dots x^{-2n+2}$ are the $(n-1)$ roots of the equation $1 + x + x^2 + \dots + x^{n-1} = 0$.

Hence $S = \pm \sqrt{n}$ or $\pm i\sqrt{n}$ according as $n \equiv 1$ or $3 \pmod 4$: and it only remains to determine the signs of the ambiguities.

Now $x^h - x^{-h} = 2i \sin \frac{2h\pi}{n}$: therefore

$$S = 2^{\frac{1}{2}(n-1)}\, i^{\frac{1}{2}(n-1)} \prod_h \sin \frac{2h\pi}{n} \quad [h = 1, 3, 5, \dots (n-2)].$$

First, suppose $n \equiv 1 \pmod 4$: then the values of h which make $\sin \frac{2h\pi}{n}$ negative are

$$\tfrac{1}{2}(n+1),\ \tfrac{1}{2}(n+5), \dots (n-2),$$

that is, $\frac{1}{4}(n-1)$ values in all; and the sign of S is the same as that of

$$(-1)^{\frac{1}{4}(n-1)} . (-1)^{\frac{1}{4}(n-1)} = +1,$$

so that $S = +\sqrt{n}$.

On the other hand if $n \equiv 3 \pmod 4$ the values of h which make $\sin \frac{2h\pi}{n}$ negative are

$$\tfrac{1}{2}(n+3),\ \tfrac{1}{2}(n+7), \dots (n-2),$$

that is, there are $\frac{1}{4}(n-3)$ values in all. Hence $S = iS'$, where the sign of S' is the same as that of

$$(-1)^{\frac{1}{4}(n-3)} . (-1)^{\frac{1}{4}(n-3)} = +1;$$

consequently $S = +i\sqrt{n}$.

Gauss proceeds to find the value of S when n is even: this part of his investigation will be omitted here, because it is much simpler to proceed as in the latter part of Dirichlet's proof given above.

191. A very interesting application of the theory is the new proof which it affords of the law of quadratic reciprocity. Gauss has given a more general theorem of which the law of reciprocity is a particular case: the proof which will be given here is taken from Dirichlet (*Zahlentheorie*, 3rd ed. p. 297).

Suppose that in the preceding formulæ n is an odd prime p: then we have

$$\phi(1, p) = \Sigma e^{2s^2\pi i/p} = i^{\frac{1}{4}(p-1)^2}\sqrt{p}.$$

We may also write

$$\phi(1, p) = 1 + 2\Sigma e^{2a\pi i/p},$$

where the summation extends to the $\frac{1}{2}(p-1)$ quadratic residues of p which are positive and less than p. Moreover, if β stands for any one of the $\frac{1}{2}(p-1)$ non-residues of p,

$$1 + \Sigma e^{2\alpha\pi i/p} + \Sigma e^{2\beta\pi i/p} = 0,$$

and hence
$$\phi(1, p) = \Sigma e^{2\alpha\pi i/p} - \Sigma e^{2\beta\pi i/p}.$$

In the same way

$$\phi(h, p) = \Sigma e^{2h\alpha\pi i/p} - \Sigma e^{2h\beta\pi i/p}.$$

Now if hRp, $h\alpha Rp$ and $h\beta Np$: while if hNp, $h\alpha Np$, $h\beta Rp$: therefore

$$\phi(h, p) = (h|p)\,\phi(1, p) = (h|p)\, i^{\frac{1}{4}(p-1)^2}\sqrt{p}.$$

Hence if q is, like p, an odd prime,

$$\phi(q, p) = (q\,|\,p)\, i^{\frac{1}{4}(p-1)^2}\sqrt{p},$$
$$\phi(p, q) = (p\,|\,q)\, i^{\frac{1}{4}(q-1)^2}\sqrt{q}.$$

Also by Art. 186,

$$\phi(q, p)\,\phi(p, q) = \phi(1, pq)$$
$$= i^{\frac{1}{4}(pq-1)^2}\sqrt{pq}.$$

Therefore
$$(p\,|\,q)(q\,|\,p) = i^{\lambda},$$

where
$$\begin{aligned}\lambda &= \tfrac{1}{4}\{(pq-1)^2 - (p-1)^2 - (q-1)^2\}\\ &= \tfrac{1}{4}\{(p^2-1)(q^2-1) - 2(p-1)(q-1)\}\\ &= \tfrac{1}{4}(p-1)(q-1)\{(p+1)(q+1) - 2\}\\ &\equiv \tfrac{1}{2}(p-1)(q-1) \pmod{4}.\end{aligned}$$

Consequently
$$(p\,|\,q)(q\,|\,p) = i^{\frac{1}{2}(p-1)(q-1)}$$
$$= (-1)^{\frac{1}{4}(p-1)(q-1)},$$

which is the law of reciprocity for two odd primes.

With regard to the supplementary formulæ, we have

$$\phi(-1, p) = (-1\,|\,p)\, i^{\frac{1}{4}(p-1)^2}\sqrt{p},$$

while, by definition,

$$\phi(-1, p) = \Sigma e^{-2s^2\pi i/p},$$

which may be obtained from $\phi(1, p)$ by changing i into $-i$. Hence

$$(-i)^{\frac{1}{4}(p-1)^2}\sqrt{p} = (-1\,|\,p)\, i^{\frac{1}{4}(p-1)^2}\sqrt{p},$$

and therefore
$$(-1\,|\,p) = (-1)^{\frac{1}{4}(p-1)^2} = (-1)^{\frac{1}{2}(p-1)}.$$

In order to determine $(2\,|\,p)$, we observe that

$$\phi(8, p)\,\phi(p, 8) = \phi(1, 8p).$$

Now $$\phi(8, p) = (8 \mid p)\,\phi(1, p) = (2 \mid p)\,\phi(1, p),$$
$$\phi(1, 8p) = (1+i)\sqrt{8p} = 4e^{\frac{1}{4}\pi i}\sqrt{p},$$
while the value of $\phi(p, 8)$ will depend on the residue of p, mod 8. By putting $p = 1, 3, 5, 7$ successively it is easily found that[1]
$$\phi(p, 8) = 4e^{p\pi i/4} = 4i^{\frac{1}{2}(p-1)} \,.\, e^{\frac{1}{4}\pi i};$$
hence, on substitution,
$$i^{\frac{1}{2}(p-1)} \,.\, (2 \mid p)\,\phi(1, p) = \sqrt{p} = i^{-\frac{1}{4}(p-1)^2}\,\phi(1, p),$$
or $$(2 \mid p) = i^{-\frac{1}{4}(p^2-1)} = (-1)^{\frac{1}{8}(p^2-1)},$$
which agrees with the result previously obtained (Art. 38).

192. Gauss's more general theorem is as follows:

If n is the product of the positive odd primes a, b, c, etc., no two of which are equal, and if m is the number of these primes which are of the form $4k+3$, then the number of the primes $a, b, c \ldots$ of which $n/a, n/b, n/c \ldots$ respectively are non-residues will be even if $m \equiv 0$ or $1 \pmod 4$, and odd if $m \equiv 2$ or $3 \pmod 4$.

For instance if $n = 3 \,.\, 5 \,.\, 7 \,.\, 11 \,.\, 13$, we have $5 \,.\, 7 \,.\, 11 \,.\, 13\, R\, 3$, $3 \,.\, 7 \,.\, 11 \,.\, 13\, N\, 5$, $3 \,.\, 5 \,.\, 11 \,.\, 13\, N\, 7$, $3 \,.\, 5 \,.\, 7 \,.\, 13\, R\, 11$, $3 \,.\, 5 \,.\, 7 \,.\, 11\, N\, 13$: the number of non-residues is 3, which is odd, in accordance with the theorem, since $m = 2$.

The proof is easy; let $aa' = bb' = cc' = \ldots = n$, then since a is prime to b,
$$\phi\left(\frac{n}{a}, a\right)\phi\left(\frac{n}{b}, b\right) = \phi\left(\frac{n}{ab} \,.\, b,\ a\right)\phi\left(\frac{n}{ab} \,.\, a,\ b\right)$$
$$= \phi\left(\frac{n}{ab},\ ab\right), \text{ by Art. 186};$$
hence $$\phi\left(\frac{n}{a}, a\right)\phi\left(\frac{n}{b}, b\right)\phi\left(\frac{n}{c}, c\right) = \phi\left(\frac{n}{abc},\ abc\right),$$
and so on: finally
$$\phi(1, n) = \Pi\phi(a', a) = \Pi(a' \mid a)\,\phi(1, a)$$
$$= i^m\,\Pi(a' \mid a)\,\Pi\sqrt{a} = i^m\sqrt{n}\,\Pi(a' \mid a),$$
because $\phi(1, a) = \sqrt{a}$ or $i\sqrt{a}$ according as $a \equiv 1$ or $3 \pmod 4$.

[1] By a slight oversight, the value of $\phi(p, 8)$ is erroneously stated in the *Zahlentheorie* to be $4e^{\frac{1}{4}\pi i}$.

On the other hand $n\equiv 1$ or $3 \pmod 4$ according as m is even or odd, so that

$$\phi(1, n) = i^{m^2}\sqrt{n};$$

hence

$$\Pi(a' \mid a) = i^{m^2-m},$$

from which the theorem immediately follows.

193. If p, as before, is an odd prime, and if X, as usual, denotes the polynomial $(x^p-1)/(x-1)$, there is a remarkable transformation of X which may be expressed by the identity

$$4X = Y^2 - (-1)^{\frac{1}{2}(p-1)}pZ^2,$$

where Y, Z are polynomials in x with integral coefficients.

To prove this, let

$$X_1 = (x-r)(x-r^{g^2})(x-r^{g^4})\ldots(x-r^{g^{p-3}}),$$
$$X_2 = (x-r^g)(x-r^{g^3})(x-r^{g^5})\ldots(x-r^{g^{p-2}});$$

then if η_0, η_1 are the roots of the period equation

$$\eta^2 + \eta + \frac{1-(-1)^{\frac{1}{2}(p-1)}p}{4} = 0,$$

X_1 is a polynomial of which the coefficients are symmetric functions of those roots of $X=0$ the sum of which makes up η_0. Hence (Art. 180) the coefficients may all be reduced to the form $a+b\eta_0$ where a, b are integers: therefore we have identically

$$X_1 = U + \eta_0 V,$$

where U, V are polynomials in x with integral coefficients. Changing r into r^g, we obtain

$$X_2 = U + \eta_1 V,$$

and hence, by multiplication,

$$X = X_1X_2 = U^2 + (\eta_0+\eta_1)UV + \eta_0\eta_1V^2:$$

therefore, substituting for $(\eta_0+\eta_1)$ and $\eta_0\eta_1$ their values, and multiplying by 4,

$$\begin{aligned}4X &= 4U^2 - 4UV + \{1-(-1)^{\frac{1}{2}(p-1)}p\}V^2\\ &= Y^2 - (-1)^{\frac{1}{2}(p-1)}pZ^2,\end{aligned}$$

if we put $Y = 2U - V$, $Z = V$.

For example, let $p=5$, then

$$\begin{aligned}X_1 &= (x-r)(x-r^4) = x^2 - \eta_0 x + 1,\\ X_2 &= x^2 - \eta_1 x + 1,\\ 4X &= (2x^2+x+2)^2 - 5x^2.\end{aligned}$$

Or again, if $p = 7$,

$$X_1 = (x - r)(x - r^2)(x - r^3)$$
$$= x^3 - \eta_0 x^2 + \eta_1 x - 1$$
$$= (x^3 - x - 1) - \eta_0 (x^2 + x),$$

and hence $\quad 4X = (2x^3 + x^2 - x - 2)^2 + 7(x^2 + x)^2.$

The simplest way of determining the coefficients of X_1 appears to be to calculate the values of the power-sums of its roots, and then to find the coefficients by Newton's formula. If s_h is the sum of the hth powers of the roots, it is evident that $s_h = \eta_0$ or η_1 according as hRp or hNp. Thus when $p = 13$, for which 1, 3, 4 are residues, and 2, 5 non-residues, we have

$$s_1 = s_3 = s_4 = \eta_0,$$
$$s_2 = s_5 = \eta_1 = -1 - \eta_0,$$

and hence, if $X_1 = x^6 + p_1 x^5 + p_2 x^4 + p_3 x^3 + p_4 x^2 + p_5 x + p_6,$

$$p_1 = -\eta_0,$$
$$p_2 = -\tfrac{1}{2}(s_2 + p_1 s_1) = -\tfrac{1}{2}(\eta_1 - \eta_0^2) = 2,$$
$$p_3 = -\tfrac{1}{3}(s_3 + p_1 s_2 + p_2 s_1)$$
$$= -\tfrac{1}{3}(\eta_0 - \eta_0\eta_1 + 2\eta_0) = -1 - \eta_0,$$
$$p_4 = -\tfrac{1}{4}(s_4 + p_1 s_3 + p_2 s_2 + p_3 s_1)$$
$$= -\tfrac{1}{4}(\eta_0 - \eta_0^2 + 2\eta_1 - \eta_0 - \eta_0^2)$$
$$= -\tfrac{1}{2}(\eta_1 - \eta_0^2) = 2,$$
$$p_5 = -\eta_0, \quad p_6 = 1;$$

therefore

$$U = x^6 + 2x^4 - x^3 + 2x^2 + 1,$$
$$V = -x^5 - x^3 - x,$$

and

$$Y = 2x^6 + x^5 + 4x^4 - x^3 + 4x^2 + x + 2,$$
$$Z = x^5 + x^3 + x.$$

It may be added that the coefficients of Z are always symmetrical, that is to say, the mth coefficient from the end is always the same as the mth coefficient from the beginning: the same is true for Y if $p \equiv 1 \pmod 4$, while if $p \equiv 3 \pmod 4$ the corresponding coefficients are equal and opposite. This consideration, of course, greatly shortens the work.

194. It is possible to find the values of p_1, p_2, etc. as explicit functions of p. Thus if we write $p = 2p' + 1$, $e_1 = (-1)^{p'}$, and $e_h = (h|p)$ for all integral values of h which are greater than 1, we have

$$s_h = \frac{-1 + e_h}{2} + e_h \eta_0 \quad (h > 1);$$

hence, by Newton's formula, and the equation of the periods,

$$\begin{aligned} p_1 &= -\eta_0, \\ 8p_2 &= (1 - 2e_2 + e_1 p) - 4(1 + e_2)\eta_0, \\ 24p_3 &= 3 - 3e_2 - 4e_3 + (1 + 3e_2)e_1 p \\ &\quad - (9 + 6e_2 + 8e_3 + e_1 p)\eta_0, \\ 3 \,.\, 2^7 p_4 &= -3 - 36e_2 - 32e_3 + (26 + 12e_2 + 32e_3)e_1 p + p^2 \\ &\quad - 8\{27 + 9e_2 + 8e_3 + (1 + 3e_2)e_1 p\}\eta_0, \end{aligned}$$

and so on; and if

$$Y = 2x^{p'} + c_1 x^{p'-1} + c_2 x^{p'-2} + \ldots$$

we have

$$\begin{aligned} c_1 &= 1, \\ 4c_2 &= 3 + e_1 p, \\ 8c_3 &= 5 + (1 + 2e_2)e_1 p, \\ 3 \,.\, 2^6 c_4 &= 105 + (30 + 24e_2 + 32e_3)e_1 p + p^2, \\ 3 \,.\, 2^7 c_5 &= 189 + (90 + 36e_2 + 32e_3 + 32e_2 e_3)e_1 p + (1 + 4e_2)p^2. \end{aligned}$$

The quantities e_h are periodic functions of p: thus we obtain for the coefficients c_1, c_2, c_3, etc. a certain limited number of distinct polynomials in p. For instance, if

$$p \equiv 1 \pmod{24},\ e_1 = e_2 = e_3 = 1,$$

and

$$c_4 = \frac{1}{3 \,.\, 2^6}(p^2 + 86p + 105);$$

while if $p \equiv 5 \pmod{24}$, $e_1 = 1$, $e_2 = e_3 = -1$, and

$$c_4 = \frac{1}{3 \,.\, 2^6}(p^2 - 26p + 105) = \frac{1}{3 \,.\, 2^6}(p - 5)(p - 21).$$

The values of the coefficients above given were calculated successively: it is very desirable, of course, to discover a method of writing down the general value of c_i, without having to calculate the preceding coefficients, but it is not easy to see how this can be done. We may eliminate $p_1, p_2 \ldots p_{i-1}$ from the first i of Newton's equations, and thus obtain p_i as a function of $s_1, s_2 \ldots s_i$ in the form of a determinant, but the reduction of this determinant to the form $a + b\eta_0$ is apparently impracticable when i is large.

195. It may be observed that, since p is prime,

$$x^p - 1 \equiv (x - 1)^p \pmod{p};$$

hence

$$4X \equiv 4(x - 1)^{p-1} \pmod{p},$$

and

$$Y \equiv 2(x - 1)^{\frac{1}{2}(p-1)} \pmod{p}.$$

For sufficiently small values of p, Y may be found by expanding

$2(x-1)^{\frac{1}{2}(p-1)}$ by the binomial theorem, and reducing each coefficient to its absolutely least residue (mod p). Thus, when $p = 11$,

$$\begin{aligned} Y &\equiv 2(x^5 - 5x^4 + 10x^3 - 10x^2 + 5x - 1) \\ &= 2x^5 + x^4 - 2x^3 + 2x^2 - x - 2. \end{aligned}$$

Legendre, in his *Théorie des Nombres,* erroneously stated that this rule applies to all cases; he afterwards, however, corrected his mistake. (Legendre: *Mémoire sur la détermination des fonctions Y et Z qui satisfont à l'équation* $4(x^n - 1) = (x-1)(Y^2 \pm nZ^2)$, *$n$ étant un nombre premier* $(4i \mp 1)$, Paris, Mém. Acad. Sci. xii. (1833), p. 81. Lebesgue: *Recherches sur les nombres,* Liouv. iii. (1838), p. 113.)

While Legendre's rule certainly fails for $p = 61$, and possibly for still smaller values of p, it holds good up to $p = 31$ inclusive. It may, in fact, be verified that when $p = 31$,

$$\begin{aligned} Y = {} & 2x^{15} + x^{14} - 7x^{13} - 11x^{12} + 2x^{11} + 8x^{10} - 3x^9 - 5x^8 \\ & + 5x^7 + 3x^6 - 8x^5 - 2x^4 + 11x^3 + 7x^2 - x - 2, \\ Z = {} & x^{14} + x^{13} - x^{12} - 2x^{11} + x^9 - x^8 - x^7 + x^6 - 2x^4 - x^3 + x^2 + x. \end{aligned}$$

The following table gives the values of Y and Z for all primes less than 31. The last case, $p = 29$, is due to Legendre; the others were calculated by Gauss.

p	Y	Z
3	$2x + 1$	1
5	$2x^2 + x + 2$	x
7	$2x^3 + x^2 - x - 2$	$x^2 + x$
11	$2x^5 + x^4 - 2x^3 + 2x^2 - x - 2$	$x^4 + x$
13	$2x^6 + x^5 + 4x^4 - x^3 + 4x^2 + x + 2$	$x^5 + x^3 + x$
17	$2x^8 + x^7 + 5x^6 + 7x^5 + 4x^4 + 7x^3$ $+ 5x^2 + x + 2$	$x^7 + x^6 + x^5 + 2x^4 + x^3$ $+ x^2 + x$
19	$2x^9 + x^8 - 4x^7 + 3x^6 + 5x^5 - 5x^4$ $- 3x^3 + 4x^2 - x - 2$	$x^8 - x^6 + x^5 + x^4 - x^3 + x$
23	$2x^{11} + x^{10} - 5x^9 - 8x^8 - 7x^7 - 4x^6$ $+ 4x^5 + 7x^4 + 8x^3 + 5x^2 - x - 2$	$x^{10} + x^9 - x^7 - 2x^6 - 2x^5$ $- x^4 + x^2 + x$
29	$2x^{14} + x^{13} + 8x^{12} - 3x^{11} + x^{10} - 2x^9$ $+ 3x^8 + 9x^7 + 3x^6 - 2x^5 + x^4$ $- 3x^3 + 8x^2 + x + 2$	$x^{13} + x^{11} - x^{10} + x^8 + x^7$ $+ x^6 - x^4 + x^3 + x$

By putting $x=1$ in the identity $4X = Y^2 \pm pZ^2$, we obtain a representation of $4p$ in the form

$$4p = m^2 \pm pn^2.$$

Thus for $p = 17$, we have

$$68 = 34^2 - 17 \,.\, 8^2$$

and so on. It may be noticed that when $p \equiv 3 \pmod{4}$ this process only leads to the trivial result

$$4p = 0^2 + p \,.\, 2^2,$$

except when $p = 3$.

196. When $p = 3n+1$ there will be a set of three periods η_0, η_1, η_2, which are the roots of a cubic equation

$$\eta^3 + c_1\eta^2 + c_2\eta + c_3 = 0,$$

where c_1, c_2, c_3 are integers which have to be determined.

If g is any primitive root of p, and $r = e^{2\pi i/p}$ as usual, we may put

$$\eta_0 = \Sigma r^{g^{3h}}, \quad \eta_1 = \Sigma r^{g^{3h+1}}, \quad \eta_2 = \Sigma r^{g^{3h+2}}.$$

All numbers prime to p may be distributed into three classes A, B, C according as their indices to the base g are congruent to 0, 1 or 2 (mod. 3). Numbers of the class A will be denoted by α, α'... and in the same way β and γ (accented if necessary) may be used to indicate numbers belonging to B and C respectively.

With this notation we may write

$$\eta_0 = \Sigma r^{\alpha}, \quad \eta_1 = \Sigma r^{\beta}, \quad \eta_2 = \Sigma r^{\gamma},$$

where the summations apply to n incongruent values (mod. p) of α, β, γ respectively.

The class A includes all the numbers which are cubic residues of p, and is the same whatever primitive root g may be chosen; if instead of g we take a primitive root g' such that $\text{ind}_{g'}, g \equiv 2$ (mod. 3) the classes B and C will be interchanged.

We observe that 1 and $p - 1 \equiv -1$ both belong to the class A. Also the product of any two numbers of the class A is a number of the same class, or, in symbols,

$$\alpha\alpha' = \alpha''.$$

In particular, $p - \alpha$, or $-\alpha$ belongs to A.

Similarly
$$\begin{array}{lll} \alpha\beta = \beta', & \beta\beta' = \gamma, & \\ & & \beta\gamma = \alpha. \\ \alpha\gamma = \gamma', & \gamma\gamma' = \beta, & \end{array}$$

Returning now to the equation of the periods, we find at once

$$c_1 = -(\eta_0 + \eta_1 + \eta_2) = 1.$$

The value of c_2 is $c_2 = \eta_0\eta_1 + \eta_1\eta_2 + \eta_2\eta_0$

$$= \Sigma\,(r^{\alpha+\beta} + r^{\beta+\gamma} + r^{\gamma+\alpha}).$$

Now the congruence

$$\alpha + \beta \equiv 0 \pmod{p}$$

is impossible, because it would lead to

$$\beta \equiv -\alpha,$$

and hence β would belong to the class A, contrary to definition. In the same way it may be inferred that the congruences $\beta + \gamma \equiv 0$, $\gamma + \alpha \equiv 0$ are impossible. Hence of the $3n^2$ terms of which

$$\Sigma\,(r^{\alpha+\beta} + r^{\beta+\gamma} + r^{\gamma+\alpha})$$

consists not one reduces to unity. But we know that the expression is a rational integer: hence its value is $(r + r^2 + \ldots + r^{p-1})$, or -1, taken $3n^2/(p-1) = n$ times. Therefore

$$c_2 = -n = -\tfrac{1}{3}(p-1).$$

The value of the remaining coefficient is

$$c_3 = -\eta_0\eta_1\eta_2 = -\Sigma r^{\alpha+\beta+\gamma}.$$

Suppose that λ denotes the number of distinct solutions of the congruence

$$\alpha + \beta + \gamma \equiv 0 \pmod{p};$$

then by the argument used in finding the value of c_2 it follows that

$$c_3 = \lambda - \frac{n^3 - \lambda}{3n},$$

so that c_3 is determined when λ is known.

Now α may assume any one of n incongruent values: suppose α' to be any one of these. Then if α'' is determined so that $\alpha'\alpha'' \equiv 1$, the congruence $\alpha' + \beta + \gamma \equiv 0$ is equivalent to

$$\alpha''(\alpha' + \beta + \gamma) \equiv 0,$$

or

$$1 + \beta' + \gamma' \equiv 0,$$

where β', γ' belong to B, C respectively. Conversely, from every solution of $1 + \beta' + \gamma' \equiv 0$ may be deduced a solution of $\alpha' + \beta + \gamma \equiv 0$, by putting $\beta \equiv \alpha'\beta'$, $\gamma \equiv \alpha'\gamma'$. Hence if the symbol (12) is used to denote the number of solutions of

$$1 + \beta + \gamma \equiv 0,$$

we have

$$\lambda = (12)\,n$$

and

$$c_3 = \tfrac{1}{3}\{(12)\,p - n^2\},$$

so that everything depends upon finding the value of (12).

To do this we consider the system of congruences given in the following table, in which the symbol placed to the left of each congruence denotes the number of distinct solutions of which it is capable.

$$\begin{array}{llllll}
(00) & 1+\alpha+\alpha'\equiv 0, & (10) & 1+\beta+\alpha\equiv 0, & (20) & 1+\gamma+\alpha\equiv 0, \\
(01) & 1+\alpha+\beta\equiv 0, & (11) & 1+\beta+\beta'\equiv 0, & (21) & 1+\gamma+\beta\equiv 0, \\
(02) & 1+\alpha+\gamma\equiv 0, & (12) & 1+\beta+\gamma\equiv 0, & (22) & 1+\gamma+\gamma'\equiv 0.
\end{array}$$

It is obvious that $(01)=(10)$, $(02)=(20)$, $(12)=(21)$; in fact, the double notation is only used for the sake of symmetry.

If we multiply the congruence

$$1+\alpha+\beta\equiv 0$$

by a number γ such that $\beta\gamma\equiv 1$, and put $\gamma\alpha=\gamma'$, we obtain $1+\gamma+\gamma'\equiv 0$. Therefore every solution of $1+\alpha+\beta\equiv 0$ is associated with one of $1+\gamma+\gamma'\equiv 0$; and in the same way from every solution of $1+\gamma+\gamma'\equiv 0$ we can deduce one of $1+\alpha+\beta\equiv 0$.

Hence $$(01)=(22),$$

and similarly $$(02)=(11).$$

Thus the matrix

$$\begin{vmatrix} (00), & (01), & (02) \\ (10), & (11), & (12) \\ (20), & (21), & (22) \end{vmatrix}$$

is reduced to the type $$\begin{vmatrix} h & j & k \\ j & k & l \\ k & l & j \end{vmatrix},$$

where h, j, k, l have still to be determined.

The series $$1,\ 2,\ 3\ldots(p-1)$$

contains n numbers α, and each of these, except the last, namely $p-1$, is followed by a number $\alpha+1$ which must belong to one of the classes A, B, C, and is therefore of the form $p-\alpha'$, $p-\beta'$, or $p-\gamma'$; that is, to every value of α, with one exception, corresponds a solution of one of the congruences

$$1+\alpha+\alpha'\equiv 0, \qquad 1+\alpha+\beta'\equiv 0, \qquad 1+\alpha+\gamma'\equiv 0.$$

Hence $$(00)+(01)+(02)=n-1,$$

or $$h+j+k=n-1\ldots\ldots\ldots\ldots(1);$$

and in the same way $$j+k+l=n\ldots\ldots\ldots\ldots(2),$$

because every number β, without exception, is followed by another number of the series.

There is yet another relation connecting h, j, k, l which may be found in the following way.

Consider the congruence

$$\alpha+\beta+\gamma+1 \equiv 0.$$

There are $(00)=h$ values of α which make $\alpha+1=\alpha'$, and the congruence

$$\alpha'+\beta+\gamma \equiv 0$$

when α' is fixed, has $(12)=l$ solutions. Thus there are hl solutions of $\alpha+\beta+\gamma+1 \equiv 0$ for which $\alpha+1=\alpha'$. Similarly there are $(01)(01)=j^2$ solutions for which $\alpha+1=\beta'$, and $(02)(02)=k^2$ solutions for which $\alpha+1=\gamma'$. Altogether there are

$$hl+j^2+k^2$$

solutions of the congruence.

But if we begin with β instead of α we find in the same way that there are $(10)(02)=jk$ solutions for which $\beta+1=\alpha'$, $(11)(12)=kl$ solutions for which $\beta+1=\beta'$, and $(12)(01)=lj$ solutions for which $\beta+1=\gamma'$. Therefore altogether there are $jk+kl+lj$ solutions; and since this must be the same as before,

$$hl+j^2+k^2=jk+kl+lj \text{ ....}(3).$$

Now from (1) and (2),

$$h=l-1,$$

and on substituting this in (3) and transposing, we find

$$l=j^2+k^2+l^2-jk-kl-lj.$$

This relation may be written in the following form:

$$12(j+k+l)+4=36(j^2+k^2+l^2-jk-kl-lj)$$
$$+12(j+k)-24l+4$$
$$=(6l-3j-3k-2)^2+27(j-k)^2,$$

that is $$4p=a^2+3b^2 \text{ ....}(4),$$

if we put $$6l-3j-3k-2=a \text{ ....}(5),$$

$$3(j-k)=b \text{ ....}(6).$$

Now it follows from the theory of binary quadratic forms for the determinant -3 that, when p is given, the values of a^2 and b^2 for which $4p=a^2+3b^2$ and $b \equiv 0 \pmod 3$ are uniquely determinate; hence the values of a and b in equations (5) and (6) are determined except as to sign. The sign of b will depend upon the choice of the primitive root g, because if the classes B and C

are interchanged so will be j and k. However, for our present purpose we shall not require b, and equation (5) shows that a is that value of $\pm\sqrt{a^2}$ which is of the form $3a'-2$.

Putting $a=3a'-2$, we find by (5)

$$2l=a'+j+k$$
$$=a'+n-l \text{ by (2).}$$

Therefore $$l=\tfrac{1}{3}(a'+n);$$

and on substituting this in the expression previously obtained for c_3 we find

$$c_3=\tfrac{1}{3}(lp-n^2)=\tfrac{1}{9}\{(a'+n)p-3n^2\}$$
$$=\tfrac{1}{9}(pa'+n).$$

Finally, therefore, the cubic equation of the periods is

$$\eta^3+\eta^2-\tfrac{1}{3}(p-1)\eta-\tfrac{1}{9}\left(pa'+\frac{p-1}{3}\right)=0,$$

which may also be written in the form

$$(3\eta+1)^3-3p(3\eta+1)-pa=0.$$

Example. Let $p=31$; then $4p=124=16+3.36$, $a=4$, and the equation in η is

$$\eta^3+\eta^2-10\eta-8=0,$$

or $$(3\eta+1)^3-93(3\eta+1)-124=0.$$

197. If we write, in the cubic equation of the periods,

$$3\eta+1=z,$$

it becomes $$z^3-3pz-pa=0;$$

and if we now put $z=2\sqrt{p}\cos\phi$, this becomes

$$2p\sqrt{p}(4\cos^3\phi-3\cos\phi)-pa=0,$$

whence $$\cos 3\phi=a/2\sqrt{p}.$$

Suppose that ϕ is the least positive value of ϕ which satisfies this equation, then the three values of z will be

$$z=2\sqrt{p}\cos\phi,\quad z'=2\sqrt{p}\cos\left(\phi+\frac{2\pi}{3}\right),\quad z''=2\sqrt{p}\cos\left(\phi+\frac{4\pi}{3}\right).$$

It is easily seen, geometrically, that z lies between $\sqrt{p}$ and $2\sqrt{p}$, z' between $-2\sqrt{p}$ and $-\sqrt{p}$, z'' between $-\sqrt{p}$ and $\sqrt{p}$.

One of the values of z is $z_0=1+3\eta_0$; to discover which it is, when p is given, is a problem which appears to be of extreme difficulty, and has not yet found an entirely satisfactory solution. Kummer, however, has given a criterion for distinguishing the roots, which is of considerable interest; and before postponing, for the present, further applications of the circular functions to arithmetic, a short account of Kummer's investigation may be given.

Let $\rho = e^{2\pi i/3} = \dfrac{-1+i\surd 3}{2}$, and let m be any number prime to p; then by an extension of the Legendre-Jacobi symbol $(m|p)$, we shall put $(m|p)_3 = 1$, ρ or ρ^2, according as the index of m to any primitive root g, taken as a base, is congruent to 0, 1 or 2 to modulus 3; in other words, $(m|p)_3 = \rho^{\text{ind}\, m}$. The expression $(m|p)_3$ may be called the cubic character of m with respect to p. If m is a cubic residue of p, that is, if the congruence $x^3 \equiv m \pmod p$ admits of solution, we have $(m|p)_3 = 1$; if otherwise, the character $(m|p)_3$ may be ρ or ρ^2 according to the primitive root taken as base.

Since the Legendrian symbol proper will not be required in what follows, the suffix will be omitted, and $(m|p)$ will be written instead of $(m|p)_3$. It is convenient also to put $(m|p)=0$, if m is divisible by p.

It immediately follows from the definition that if $m \equiv m'$ (mod p), $(m|p) = (m'|p)$; that if m, m' are any two integers,

$$(m|p)(m'|p) = (mm'|p);$$

and that, since $-1 = (-1)^3$ is a cubic residue of p,

$$(-m|p) = (m|p).$$

As in last article, suppose $p = 3n+1$, and let the integers 1, 2, 3...$3n$ be distributed into three classes A, B, and C according as their cubic character is 1, ρ, or ρ^2. We have

$$z_0 = 1 + 3\Sigma r^\alpha,$$

$$z_1 = 1 + 3\Sigma r^\beta,$$

$$z_2 = 1 + 3\Sigma r^\gamma;$$

and hence, observing that $1+\rho+\rho^2=0$,

$$\begin{aligned} z_0 + \rho z_1 + \rho^2 z_2 &= 3\Sigma\,(r^\alpha + \rho r^\beta + \rho^2 r^\gamma) \\ &= 3\Sigma\,(h|p) r^h \\ &\quad (h = 1, 2, 3 \ldots p-1). \end{aligned}$$

Since z_0, z_1, z_2 are real, we may write

$$z_0 = 1 + 3\Sigma \cos \frac{2\alpha\pi}{p}$$

$$z_1 = 1 + 3\Sigma \cos \frac{2\beta\pi}{p}$$

$$z_2 = 1 + 3\Sigma \cos \frac{2\gamma\pi}{p};$$

and hence
$$z_0 + \rho z_1 + \rho^2 z_2 = 6\Sigma\,(k|p) \cos \frac{2k\pi}{p},$$
$$[k = 1,\ 2 \ldots \tfrac{1}{2}(p-1)]$$

since $(k|p) \cos \dfrac{2k\pi}{p}$ is not altered by changing k into $p - k$.

It is proved, in a similar way, that if m is any integer,

$$(m|p)^2 (z_0 + \rho z_1 + \rho^2 z_2) = 6 \sum_k (k|p) \cos \frac{2km\pi}{p}.$$

Suppose, now, that $f(\theta)$ is a function such that for all values of θ from 0 to π, both inclusive,

$$f(\theta) = A_1 \cos\theta + A_2 \cos 2\theta + A_3 \cos 3\theta + \ldots$$

Then

$$\Sigma\,(k|p) f\left(\frac{2k\pi}{p}\right) = A_1\,\Sigma\,(k|p)\cos\frac{2k\pi}{p} + A_2\,\Sigma\,(k|p)\cos\frac{4k\pi}{p} + \ldots$$
$$= \frac{z_0 + \rho z_1 + \rho^2 z_2}{6} \{(1|p)^2 A_1 + (2|p)^2 A_2 + \ldots\},$$

that is,
$$6 \sum_k (k|p) f\left(\frac{2k\pi}{p}\right) = (z_0 + \rho z_1 + \rho^2 z_2) \sum_s (s|p)^2 A_s,$$
$$\begin{pmatrix} k = 1,\ 2, \ldots \tfrac{1}{2}(p-1); \\ s = 1,\ 2,\ 3 \ldots \end{pmatrix}.$$

It is known that if $0 \ngtr \theta \ngtr \pi$,

$$\frac{\pi^2}{8} - \frac{\pi\theta}{4} = \cos\theta + \frac{\cos 3\theta}{3^2} + \frac{\cos 5\theta}{5^2} + \ldots$$

therefore
$$6 \sum_k (k|p)\left(\frac{\pi^2}{8} - \frac{k\pi^2}{2p}\right) = (z_0 + \rho z_1 + \rho^2 z_2) \sum_t (t|p)^2 t^{-2}$$
$$[t = 1,\ 3,\ 5 \ldots].$$

Put
$$A = \Sigma\alpha^{-2},$$
$$B = \Sigma\beta^{-2},$$
$$C = \Sigma\gamma^{-2},$$

where the summations refer to *all* positive odd integers which belong to the classes (α), (β), (γ) respectively, then

$$6\,\Sigma\,(k|p)\left(\frac{\pi^2}{8}-\frac{k\pi^2}{2p}\right)=(z_0+\rho z_1+\rho^2 z_2)\,(A+\rho^2 B+\rho C).$$

Now let $\Sigma\alpha'$ stand for the sum of all the numbers α which are positive and less than $\frac{1}{2}p$, and let $\Sigma\beta'$, $\Sigma\gamma'$ have analogous meanings. Moreover put

$$\begin{aligned}
m_0&=\tfrac{1}{3}(\Sigma\beta'+\Sigma\gamma'-2\Sigma\alpha')\\
&=\tfrac{1}{3}(\Sigma\alpha'+\Sigma\beta'+\Sigma\gamma')-\Sigma\alpha'\\
&=\tfrac{1}{24}(p^2-1)-\Sigma\alpha',\\
m_1&=\tfrac{1}{3}(\Sigma\gamma'+\Sigma\alpha'-2\Sigma\beta')=\tfrac{1}{24}(p^2-1)-\Sigma\beta',\\
m_2&=\tfrac{1}{3}(\Sigma\gamma'+\Sigma\alpha'-2\Sigma\gamma')=\tfrac{1}{24}(p^2-1)-\Sigma\gamma'.
\end{aligned}$$

Then the expression

$$\begin{aligned}
6\Sigma\,(k|p)\left(\frac{\pi^2}{8}-\frac{k\pi^2}{2p}\right)&=-\frac{3\pi^2}{p}\,\Sigma\,(k|p)\,k\\
&=-\frac{3\pi^2}{p}\,(\Sigma\alpha'+\rho\Sigma\beta'+\rho^2\Sigma\gamma')\\
&=\frac{3\pi^2}{p}\,(m_0+\rho m_1+\rho^2 m_2).
\end{aligned}$$

Therefore

$$\frac{3\pi^2}{p}\,(m_0+\rho m_1+\rho^2 m_2)=(z_0+\rho z_1+\rho^2 z_2)\,(A+\rho^2 B+\rho C).$$

In exactly the same way,

$$\frac{3\pi^2}{p}\,(m_0+\rho^2 m_1+\rho m_2)=(z_0+\rho^2 z_1+\rho z_2)\,(A+\rho B+\rho^2 C);$$

and since

$$\frac{3\pi^2}{p}\,(m_0+m_1+m_2)=0=(z_0+z_1+z_2)\,(A+B+C),$$

we have

$$\begin{aligned}
\frac{3\pi^2}{p}\,m_0&=Az_0+Bz_1+Cz_2,\\
\frac{3\pi^2}{p}\,m_1&=Az_1+Bz_2+Cz_0,\\
\frac{3\pi^2}{p}\,m_2&=Az_2+Bz_0+Cz_1.
\end{aligned}$$

The solution of these equations gives z_0, z_1, z_2 without ambiguity in terms of m_0, m_1, m_2, A, B, C. If we put

$$\Delta=A^2+B^2+C^2-BC-CA-AB,$$

an essentially positive quantity, it is found without difficulty that

$$\frac{p\Delta}{3\pi^2} z_0 = Am_0 + Cm_1 + Bm_2 = (C - A)\, m_1 + (B - A)\, m_2,$$

$$\frac{p\Delta}{3\pi^2} z_1 = Bm_0 + Am_1 + Cm_2 = (C - A)\, m_2 + (B - A)\, m_0,$$

$$\frac{p\Delta}{3\pi^2} z_2 = Cm_0 + Bm_1 + Am_2 = (C - A)\, m_0 + (B - A)\, m_1.$$

Hence also

$$\frac{p\Delta}{3\pi^2}(z_0 - z_1) = (C + A - 2B)\, m_0 - (A + B - 2C)\, m_1,$$

$$\frac{p\Delta}{3\pi^2}(z_1 - z_2) = (C + A - 2B)\, m_1 - (A + B - 2C)\, m_2,$$

$$\frac{p\Delta}{3\pi^2}(z_2 - z_0) = (C + A - 2B)\, m_2 - (A + B - 2C)\, m_0.$$

Now the quantities $A - B$, $A - C$, $A + B - 2C$, $C + A - 2B$ are all positive. We have, in fact,

$$\frac{\pi^2}{8} = 1 + \frac{1}{3^2} + \frac{1}{5^2} + \frac{1}{7^2} + \dots$$

$$= \left(1 + \frac{1}{p^2} + \frac{1}{p^4} + \dots\right) \Sigma \frac{1}{k^2},$$

where k assumes all odd values prime to p: hence

$$\frac{\pi^2}{8} = \frac{p^2}{p^2 - 1} \Sigma \frac{1}{k^2} = \frac{p^2}{p^2 - 1}(A + B + C);$$

therefore $$A + B + C = \frac{\pi^2}{8}\left(1 - \frac{1}{p^2}\right) < \frac{\pi^2}{8} < \frac{5}{4}.$$

Now $A = 1 + \frac{1}{\alpha_1{}^2} + \dots > 1$: therefore $B + C < \frac{1}{4}$, and *a fortiori* $B < \frac{1}{4}$, $C < \frac{1}{4}$; consequently

$$A - B > \tfrac{3}{4}, \quad A - C > \tfrac{3}{4}, \quad A + B - 2C > \tfrac{1}{2}, \quad C + A - 2B > \tfrac{1}{2}.$$

Since $m_0 + m_1 + m_2 = 0$, one of the three numbers m_0, m_1, m_2 must be greater than either of the rest numerically. Suppose m_0 is positive, and the greatest numerically; then m_1, m_2 are both negative, and it follows from the equations previously obtained that z_0, $z_0 - z_1$, $z_0 - z_2$ are all positive. In this case, then, z_0 is the root which lies between $\sqrt{p}$ and $2\sqrt{p}$. Similarly if m_0 is negative, and numerically greater than either m_1 or m_2, the quantities z_0, $z_0 - z_1$, $z_0 - z_2$ are all negative, and z_0 lies between $-\sqrt{p}$ and $-2\sqrt{p}$. In the same way if m_1 is numerically greater than m_0 or m_2, the limits of z_1 are determined: while if m_2 is numerically greater than m_0 or m_1, the root z_2 is known. In every case, therefore, we have a criterion to distinguish one of the three roots z_0, z_1, z_2; and since they are all expressible as rational functions of any one of them, the determination may be completely effected.

It should be observed, however, as Kummer himself remarks, that the criterion thus obtained is not really what is required. The calculation of m_0, m_1, m_2 when p is large, is very tedious, and these numbers are not connected with the value of p in any obvious or essential way. Kummer has found by actual calculation that the limits of z_0 are

$-2\sqrt{p}$ and $-\sqrt{p}$ for $p = 97$, 139, 151, 199, 211, 331, 433;

$-\sqrt{p}$ and $+\sqrt{p}$ for $p = 13$, 19, 37, 61, 109, 157, 193, 241, 283, 367, 373, 379, 397, 487;

$+\sqrt{p}$ and $+2\sqrt{p}$ for $p = 7$, 31, 43, 67, 73, 79, 103, 127, 163, 181, 223, 229, 271, 277, 307, 313, 337, 349, 409, 421, 439, 457, 463, 499.

It is very curious that the proportion of primes in the different classes is nearly that of $1:2:3$, and it is much to be desired that some simple method of discriminating the classes might be discovered.

198. The present chapter contains only a mere outline of a very extensive theory, which has not yet been by any means completed. Its importance will become even more evident in connexion with the theory of higher congruences and of algebraical integers in general; but before we enter upon this, there are various problems which may be more conveniently discussed at this stage, and among them is that of determining the number of classes of binary quadratic forms for a given determinant. To this the next chapter will be devoted.

AUTHORITIES.

In addition to the references already given, the following will be found useful :—

Gauss : *Disq. Arith.* Arts. 335--366.

Summatio quarumdam serierum singularium (Comm. Soc. Reg. Gotting. 1811).

Dirichlet : *Ueber eine neue Anwendung bestimmter Integrale auf die Summation endlicher oder unendlicher Reihen* (Abhand. d. königl. Preuss. Akad. d. Wissensch. von 1835, p. 391).

Eisenstein : *Beiträge zur Kreistheilung* (Crelle, xxvii. (1844), p. 269).

Allgemeine Untersuchungen über die Formen dritten Grades mit drei Variabeln welche der Kreistheilung ihre Entstehung verdanken (Crelle, xxviii. (1844), p. 289, xxix. p. 19).

Ueber die Irreductibilität und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt (Crelle, xxxix. (1850), p. 160).

Kronecker : *Sur les facteurs irréductibles de l'expression* x^n-1 (Liouv. xix. (1854), p. 177).

Kummer : *De residuis cubicis disquisitiones nonnullæ analyticæ* (Crelle, xxxii. (1846), p. 341).

Staudt (v.): *Ueber die Functionen Y und Z, welche der Gleichung*

$$4(x^p-1)/(x-1)=Y^2\pm pZ^2$$

Genüge leisten, wo p eine Primzahl der Form $4k\pm1$ *ist* (Crelle, lxvii. (1867), p. 205).

Stieltjes : *Contribution à la théorie des résidus cubiques et biquadratiques* (Archives Néerlandaises, xviii. (1883), p. 358). This is based upon Gauss's memoirs on biquadratic residues, which will be considered in a subsequent chapter.

Bachmann's lectures on cyclotomy (*Die Lehre von der Kreistheilung und ihre Beziehungen zur Zahlentheorie,* Leipzig, 1872) give an exceedingly clear and interesting account of the subject, with numerous references to the original sources.

CHAPTER VIII.

Determination of the Number of Properly Primitive Classes for a given Determinant.

199. The second volume of Gauss's collected works contains (p. 269) a remarkable unfinished memoir entitled *De nexu inter multitudinem classium, in quas formæ binariæ secundi gradus distribuuntur, earumque determinantem.* From this it appears that Gauss succeeded in determining the number of classes belonging to a given determinant both for definite and for indefinite forms; and with regard to definite forms it is possible to make out the method which was actually adopted. Gauss never published his investigation; in fact the first published demonstration is that of Dirichlet in his *Recherches sur diverses applications,* etc. already referred to. Dirichlet's analysis will be considered later on; in the present chapter an attempt will be made to present Gauss's method in a simplified form, and at the same time to avoid the objections on the score of deficiency in rigour, to which, as pointed out by Dedekind in his editorial notes on the memoir, Gauss's deduction appears to be liable. The materials for this simplification are mainly derived from the above-mentioned notes of Dedekind, and from Dirichlet's great memoir.

The principle of the method consists in assuming a number m which is prime to $2D$, and constructing two different expressions for the *asymptotic* value of the average number of representations of m by properly primitive forms of determinant D: that is to say, expressions which approximate to the true value when m is very large. One of these expressions involves as a factor h, the number of properly primitive classes, while the other does not; and by a comparison of the two expressions, we obtain h in the form of a semi-convergent infinite series. The semi-convergent character of this series is the principal difficulty of the investigation.

200. Definite and indefinite forms will have to be considered separately; we shall begin with the former.

Let
$$f = ax^2 + 2bxy + cy^2$$
be a positive properly primitive form of determinant
$$D = b^2 - ac = -\Delta,$$
a negative integer.

It is always possible to assign values to x and y, say $x = \xi$, $y = \eta$, prime to each other, and such that
$$a' = f(\xi, \eta) = a\xi^2 + 2b\xi\eta + c\eta^2$$
may be prime to 2Δ (cf. Art. 127).

We may suppose that a is prime to 2Δ: because if this were not the case we could find integers ξ', η', such that $\xi\eta' - \xi'\eta = 1$, and then the substitution $\begin{pmatrix} \xi, & \xi' \\ \eta, & \eta' \end{pmatrix}$ would transform f into an equivalent form $f' = (a', b', c')$ with its first coefficient prime to 2Δ.

It is clear that if $f(\xi, \eta)$ is prime to 2Δ, so is $f(2\Delta u + \xi, 2\Delta v + \eta)$, where u, v are any integers. We will suppose that ξ, η are both less than 2Δ and not negative.

We have $\quad a(a\xi^2 + 2b\xi\eta + c\eta^2) = (a\xi + b\eta)^2 + \Delta\eta^2,$
and this is prime to 2Δ if $a\xi + b\eta$ is so.

Now let β be any one of the $\phi(2\Delta)$ numbers less than 2Δ and prime to it; then if we put
$$a\xi + b\eta \equiv \beta \pmod{2\Delta},$$
any value of η comprised in the set $0, 1, 2, \ldots (2\Delta - 1)$ is associated by means of this congruence with a determinate value of ξ, which is less than 2Δ and not negative.

Since each number β thus gives rise to 2Δ pairs (ξ, η), the total number of sets (ξ, η) for which $0 \leqq \xi < 2\Delta$, $0 \leqq \eta < 2\Delta$, and $f(\xi, \eta)$ is prime to 2Δ, is
$$2\Delta\phi(2\Delta).$$

The points whose rectangular coordinates are $(2\Delta u + \xi, 2\Delta v + \eta)$ form a net, every mesh of which is a square of area $4\Delta^2$. Altogether we have $2\Delta\phi(2\Delta)$ distinct nets, the nodes of which correspond to values of (x, y) which make f prime to 2Δ.

201. Now consider the ellipse represented by the equation

$$ax^2 + 2bxy + cy^2 = m$$

where m is a large positive integer. The area of this ellipse is $\pi m/\sqrt{\Delta}$, and hence the number of nodes within the curve which belong to the aforesaid networks is asymptotically

$$\frac{\pi m}{\sqrt{\Delta}} \cdot \frac{2\Delta\phi(2\Delta)}{4\Delta^2} = \frac{\pi m\phi(2\Delta)}{2\Delta\sqrt{\Delta}};$$

that is to say, its value is $\pi m\phi(2\Delta)/2\Delta\sqrt{\Delta} + \epsilon$, where ϵ/m ultimately vanishes, when m increases indefinitely.

Suppose that $m_1, m_2, \ldots m_\mu$ are the positive integers less than m and prime to 2Δ; and let $\theta(m_i)$ denote the number of distinct representations of m_i by the form (a, b, c); then the number of which the asymptotic value has just been found is rigorously

$$\theta(m_1) + \theta(m_2) + \ldots + \theta(m_\mu).$$

If we take a representative form from each of the positive properly primitive classes, say $f_1, f_2, \ldots f_h$, and if we construct the ellipses

$$f_1 = m, \quad f_2 = m, \ldots f_h = m,$$

(all of which have the same area $\pi m/\sqrt{\Delta}$), then the number of nodes included by all the ellipses, counting each node once for every ellipse within which it lies, is asymptotically

$$\frac{h\pi m\phi(2\Delta)}{2\Delta\sqrt{\Delta}}.$$

On the other hand, this number is rigorously

$$\sum_k \sum_i \theta_k(m_i) \quad \begin{pmatrix} i = 1, 2, 3 \ldots \mu \\ k = 1, 2, 3 \ldots h \end{pmatrix},$$

where $\theta_k(m_i)$ denotes the number of distinct representations of m_i by the form f_k.

If we write $\psi(m)$ for μ, the number of integers less than m and prime to 2Δ, we have

$$\frac{m}{\psi(m)} \cdot \frac{h\pi\phi(2\Delta)}{2\Delta\sqrt{\Delta}} = \frac{1}{\psi(m)} \Sigma\Sigma\theta_k(m_i),$$

ultimately, when m is infinite.

Now it is easily seen that

$$\underset{m=\infty}{\text{Lt}} \cdot \frac{\psi(m)}{m} = \frac{\phi(2\Delta)}{2\Delta};$$

hence ultimately,

$$\frac{h\pi}{\sqrt{\Delta}} = \underset{m=\infty}{\mathrm{Lt}} \cdot \frac{1}{\psi(m)} \Sigma\Sigma\theta_k(m_i) \ldots\ldots\ldots\ldots\ldots(\mathrm{A}),$$

and we have to calculate the value of the expression on the right hand.

202. In order to find representations of m_i by forms of determinant D, we have first to solve the congruence

$$n^2 \equiv D \pmod{m_i}$$

and then to every solution will correspond a form (m_i, n, l) which belongs to a class every form of which will represent m_i.

Each solution of the congruence gives rise to a group of primitive representations by each form of the corresponding class: and the number of these groups is equal to the number of the solutions of the congruence. (Cf. Arts. 59, 90.)

But by Art. 35, if $p, q, r\ldots$ are the t different prime factors of m_i, which by supposition are all odd, the number of solutions is 0 or 2^t according as D is not or is a quadratic residue of each of the primes. In every case, the number of solutions may be written in the form

$$\{1+(D|p)\}\{1+(D|q)\}\ldots = \Pi\{1+(D|p)\},$$

where the product extends to all prime factors of m_i.

Call this number $\chi(m_i)$; then, making use of Jacobi's extension of Legendre's symbol, we have

$$\begin{aligned}\chi(m_i) &= 1 + (D|p) + (D|q) + \ldots\\ &\quad + (D|pq) + \ldots\\ &= \Sigma(D|\delta'),\end{aligned}$$

where the summation extends to all divisors of m_i which involve no square factor.

If ϵ is the number of solutions of the Pellian equation $T^2 - DU^2 = 1$, each form by which m_i can be represented at all gives rise to ϵ distinct primitive representations, which form a group. When D is negative $\epsilon = 2$, except when $D = -1$, in which case $\epsilon = 4$.

Suppose now that λ^2 is any square divisor of m_i. Then the congruence

$$n^2 \equiv D \pmod{m_i/\lambda^2},$$

has $\chi(m_i/\lambda^2)$ solutions, each of which gives ϵ primitive representations of m_i/λ^2, and therefore ϵ representations of m_i for which $dv(x, y) = \lambda$.

Now if δ'' is any divisor of m_i/λ^2 which has no square factor,

$$\chi(m_i/\lambda^2) = \Sigma(D|\delta'')$$
$$= \Sigma(D|\delta''\lambda^2),$$

since $(D|\lambda^2) = 1$.

Every divisor of m_i can be expressed in the form $\delta''\lambda^2$, where δ'' involves no square factor, and therefore, on the whole, the number of representations of m_i, both primitive and derived, is

$$\epsilon\Sigma(D|\delta),$$

where the summation extends to all divisors of m_i.

But this is also what was previously denoted by

$$\theta_1(m_i) + \theta_2(m_i) + \ldots + \theta_h(m_i),$$

so that the double sum which occurs in equation (A) may be written

$$\Sigma\Sigma\theta_k(m_i) = \epsilon\sum_{m_i}\sum_{\delta}(D|\delta) \ldots\ldots\ldots\ldots\ldots\ldots\ldots (B).$$

203. Henceforward we shall write 2 instead of ϵ, it being understood that 2 must be replaced by 4 when $D = -1$.

Every number which is less than m and prime to 2Δ will occur in (B) as a divisor δ. Let n be any one of these; then the symbol $(D|n)$ will occur in (B) as often as there are multiples of n which are less than m and prime to 2Δ. Let $[m/n]$ be the integer next less than m/n; then the number of times $(D|n)$ will occur is $\psi([m/n])$, or more simply $\psi(m/n)$, if we agree to take only the integral part of m/n.

Hence (B) is transformed into

$$\Sigma\Sigma\theta_k(m_i) = 2\Sigma\psi(m/n)(D|n),$$

and (A) becomes

$$\frac{h\pi}{\sqrt{\Delta}} = \underset{m=\infty}{\mathrm{Lt}} \,.\, 2\sum_{n}\frac{\psi(m/n)}{\psi(m)}(D|n) \ldots\ldots\ldots\ldots\ldots\ldots (C),$$

where the summation extends to all numbers n which are less than m and prime to 2Δ.

It is to be observed that $2\Sigma\psi(m/n)(D|n)$ is rigorously equal to the total number of representations of the numbers $m_1, m_2, \ldots m_\mu$ by properly primitive forms of determinant D; so that the expression on the right hand in (C) is strictly the average number of representations for one of these numbers.

So long as m is finite, it does not matter in what order the terms of the sum are arranged; and even when m becomes infinite the series must have a determinate value however the terms are taken, provided that none of them are omitted.

We shall effect the summation by supposing that the terms are arranged so that n increases continually as we go from left to right.

When m becomes indefinitely large, the sum becomes an infinite series, which may be divided into two parts, for the first of which n is very small compared with m, while for the second it is not.

So long as n is small compared with m, we have asymptotically

$$\psi(m) = \frac{m\phi(2\Delta)}{2\Delta}, \qquad \psi(m/n) = \frac{m\phi(2\Delta)}{2\Delta n},$$

and hence
$$\underset{m=\infty}{\text{Lt.}} \frac{\psi(m/n)}{\psi(m)} = \frac{1}{n}.$$

Thus the first part of the series reduces to

$$\Sigma \frac{1}{n}(D \mid n) \quad (m = \infty,\ n = \infty;\ \text{lt. } n/m = 0).$$

For the remaining part of the series we may suppose

$$\text{Lt. } (m/n) < M,$$

where M is some finite quantity; hence for the residue

$$\Sigma \frac{\psi(m/n)}{\psi(m)}(D \mid n) < \psi(M)\, \Sigma \frac{1}{\psi(m)}(D \mid n)$$
$$< \frac{\psi(M)}{\psi(m)} \Sigma (D \mid n).$$

It follows from Art. 46 that the sum of every $4\phi(\Delta)$ consecutive terms of $\Sigma(D \mid n)$, in the order written, is zero: hence the limit of $\Sigma(D \mid n)$, although indeterminate, is not infinite; and since $\psi(m)$ increases without limit, this remaining part of the series ultimately vanishes, and we have ultimately

$$\frac{h\pi}{\sqrt{\Delta}} = 2 \,.\, \Sigma \frac{1}{n}(D \mid n)$$

or
$$h = \frac{2\sqrt{\Delta}}{\pi} \Sigma \frac{1}{n}(D \mid n),$$

where, for convenience of calculation, the terms are to be written in such an order that n increases continually, and $\Sigma \frac{1}{n}(D \mid n)$ really stands for

$$\text{Lt. } \Sigma \frac{1}{n}(D \mid n),$$

where n assumes all positive integral values which are prime to 2Δ, and such that $\text{Lt}\,(n/m) = 0$, when m is increased without limit.

If $D = -1$, we must write

$$h = \frac{4}{\pi} \Sigma \frac{1}{n}(-1 \mid n).$$

As a verification, we know that in this case $h = 1$, so that we should have

$$1 = \frac{4}{\pi}\left(1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \dots\right),$$

the truth of which is well known.

204. We will now suppose that D is positive. In this case the equation $t^2 - Du^2 = 1$ has an infinite number of solutions, so that every root of the congruence $n^2 \equiv D \pmod{m}$ leads to an infinite number of representations of m by one and the same form of a particular class. It is possible, however, to assign certain conditions of inequality by means of which one of these representations may be isolated from the rest.

It has already been proved (Art. 89) that if $x = \xi$, $y = \eta$ gives a representation of m by the properly primitive form (a, b, c), then the complete set of representations may be obtained from

$$x = t\xi - u(b\xi + c\eta),$$
$$y = t\eta + u(a\xi + b\eta),$$

where (t, u) is any integral solution of $t^2 - Du^2 = 1$.

This leads to

$$\begin{aligned} ax + (b + \sqrt{D})\,y &= (t + u\sqrt{D})\,\{a\xi + (b + \sqrt{D})\,\eta\} \\ &= \pm\,(T + U\sqrt{D})^n\,\{a\xi + (b + \sqrt{D})\,\eta\}, \\ ax + (b - \sqrt{D})\,y &= \pm\,(T - U\sqrt{D})^n\,\{a\xi + (b - \sqrt{D})\,\eta\}, \end{aligned}$$

where T, U have their usual meanings, and n is any real integer.

We may suppose that a is positive, because the class to which (a, b, c) belongs will certainly contain some forms with a positive first coefficient, and it is enough to consider representations by any one form of the class.

The different values of $ax+(b+\surd D)\,y$, taken without regard to sign, form a geometrical progression, extending to infinity both ways, of which the common ratio is $T+U\surd D$. Writing θ for this ratio, it will be possible, in one way only, to choose the sign of the ambiguity, and an integral value of n, so that

$$\sqrt{am} < ax+(b+\surd D)\,y < \theta\sqrt{am},$$

and in this way a particular solution is isolated from all the rest of the same set.

Observing that $\{ax+(b+\surd D)\,y\}\,\{ax+(b-\surd D)\,y\} = am$, we see that it follows from the above inequalities that

$$\sqrt{am} > ax+(b-\surd D)\,y > \theta^{-1}\sqrt{am};$$

and by combining these results we infer successively

$$y > 0$$

and $$\theta\,\{ax+(b-\surd D)\,y\} - \theta^{-1}\,\{ax+(b+\surd D)\,y\} > 0,$$

or $$(\theta-\theta^{-1})\,(ax+by) - (\theta+\theta^{-1})\,y\surd D > 0,$$

which reduces to

$$U\,(ax+by) - Ty > 0.$$

Conversely, if the conditions

$$y > 0, \qquad U\,(ax+by) - Ty > 0,$$

are satisfied, it will follow that

$$\sqrt{am} < ax+(b+\surd D)\,y < \theta\sqrt{am};$$

because we have at once

$$U\,\{ax+(b+\surd D)\,y\} > \theta y > 0,$$

$$ax+(b+\surd D)\,y > ax+(b-\surd D)\,y > \frac{am}{ax+(b+\surd D)\,y},$$

whence $$ax+(b+\surd D)\,y > \sqrt{am};$$

while since

$$\theta\,\{ax+(b-\surd D)\,y\} - \theta^{-1}\,\{ax+(b+\surd D)\,y\} > 0,$$

we have, by multiplying by $\theta\,\{ax+(b+\surd D)\,y\}$, which is positive,

$$\theta^2 am - \{ax+(b+\surd D)\,y\}^2 > 0,$$

and therefore $$ax+(b+\surd D)\,y < \theta\sqrt{am}.$$

205. Consider, now, the hyperbolic sector enclosed by

$$ax^2+2bxy+cy^2 = m,$$

$$y = 0,$$

$$U\,(ax+by) - Ty = 0.$$

By changing to polar coordinates, it is easily found that the area of the sector is

$$A = \frac{m}{2}\int_0^\alpha \frac{d\theta}{a\cos^2\theta + 2b\cos\theta\sin\theta + c\sin^2\theta},$$

where α is the least positive angle for which

$$U(a\cot\alpha + b) - T = 0.$$

Hence
$$A = \frac{m}{4\sqrt{D}}\left[\log\frac{a\cot\theta + b + \sqrt{D}}{a\cot\theta + b - \sqrt{D}}\right]_0^\alpha$$
$$= \frac{m}{4\sqrt{D}}\log\frac{T + U\sqrt{D}}{T - U\sqrt{D}}$$
$$= \frac{m}{2\sqrt{D}}\log(T + U\sqrt{D}),$$

since
$$T^2 - DU^2 = 1.$$

The argument now proceeds exactly as in the case of definite forms, except that instead of a number of equal ellipses we have a number of equal hyperbolic sectors. Thus equation (A) of Art. 201 is replaced by

$$\frac{h}{2\sqrt{D}}\log(T + U\sqrt{D}) = \underset{m=\infty}{\mathrm{Lt}} \cdot \frac{1}{\psi(m)}\Sigma\Sigma\theta_k(m_i),$$

and the final result is

$$h = \frac{2\sqrt{D}}{\log(T + U\sqrt{D})}\Sigma\frac{1}{n}(D \mid n),$$

where h is the number of properly primitive classes of determinant D, and the summation applies to all positive integers prime to $2D$.

As a verification, suppose $D = 3$; here $h = 2$, the representative forms being $(1, 0, -3)$, $(-1, 0, 3)$. We have $T = 2$, $U = 1$, and the series $\Sigma\frac{1}{n}(D \mid n)$ is

$$S = 1 - \frac{1}{5} - \frac{1}{7} + \frac{1}{11} + \frac{1}{13} - \frac{1}{17} - \frac{1}{19} + \dots$$
$$= \sum_0^\infty\left\{\frac{1}{12n+1} - \frac{1}{12n+5} - \frac{1}{12n+7} + \frac{1}{12n+11}\right\}.$$

It ought, therefore, to be true that

$$S = \frac{1}{\sqrt{3}}\log(2 + \sqrt{3});$$

and this may be verified as follows.

Putting $e^{2\pi i/3} = \rho$, we have

$$\log\left(\frac{1-x}{1-x}\cdot\frac{1-\rho x}{1+\rho x}\right) = 2\left\{x + \frac{1}{3}x^3 + \frac{1}{5}x^5 + \dots \right.$$

$$\left. - \rho x - \frac{1}{3}x^3 - \frac{1}{5}\rho^2 x^5 - \dots\right\}$$

$$= 2(1-\rho)\left\{x - \frac{1}{5}\rho^2 x^5 + \frac{1}{7}x^7 - \frac{1}{11}\rho^2 x^{11} + \dots\right\}.$$

Suppose $x = i\rho$; then

$$\log\left(\frac{1+i\rho}{1-i\rho}\cdot\frac{1-i\rho^2}{1+i\rho^2}\right) = 2i\rho(1-\rho)\left\{1 - \frac{1}{5} - \frac{1}{7} + \frac{1}{11} - \dots\right\}$$

$$= 2i\rho(1-\rho)S.$$

Now

$$\frac{(1+i\rho)(1-i\rho^2)}{(1-i\rho)(1+i\rho^2)} = \frac{2+(2\rho+1)i}{2-(2\rho+1)i} = \frac{2-\sqrt{3}}{2+\sqrt{3}} = \frac{1}{(2+\sqrt{3})^2};$$

and $\qquad 2i\rho(1-\rho) = 2i(2\rho+1) = -2\sqrt{3}$;

therefore $\qquad -2S\sqrt{3} = \log(2+\sqrt{3})^{-2} = -2\log(2+\sqrt{3})$,

or $$S = \frac{1}{\sqrt{3}}\log(2+\sqrt{3}),$$

which is right.

206. It will now be shown that the series

$$H = \Sigma\frac{1}{n}(D\,|\,n),$$

upon which the determination of h has been made to depend, may be expressed in finite terms. It will be supposed that D is not divisible by any square, since by Art. 151 the class-number for a determinant DS^2 may be deduced from that for the determinant D. We shall therefore have to consider the cases when $D = \pm P$ or $\pm 2P$, P being the product of different positive odd primes; it will further be necessary to distinguish each case according as $P \equiv 1$ or $3 \pmod 4$. Altogether, then, there will be eight different cases.

I. Suppose $\qquad \boldsymbol{D = -P \equiv 1 \pmod 4}$.

By the generalized law of reciprocity

$$(D\,|\,n) = (-P\,|\,n) = (n\,|\,P),$$

so that $$H = \Sigma\frac{1}{n}(n\,|\,P).$$

Since $(n' \mid P) = (n \mid P)$ if $n' \equiv n \pmod{2P}$, and $(n' \mid P) = -(n \mid P)$ if $n' \equiv -n \pmod{2P}$, it follows that

$$H = \Sigma\,(\nu \mid P)\left\{\frac{1}{\nu} - \frac{1}{2P-\nu} + \frac{1}{2P+\nu} - \frac{1}{4P-\nu} + \frac{1}{4P+\nu} - \dots\right\},$$

where the summation applies to all odd numbers ν which are less than P and prime to it.

Now by logarithmic differentiation of

$$\sin x = x \prod_1^\infty \left(1 - \frac{x^2}{m^2\pi^2}\right)$$

we find that
$$\cot x = \frac{1}{x} - \sum_1^\infty \frac{2x}{m^2\pi^2 - x^2}:$$

hence
$$H = \frac{\pi}{2P}\,\Sigma\,(\nu \mid P)\cot\frac{\nu\pi}{2P}.$$

This, as it stands, is a finite expression: it may, however, be transformed in such a way that the circular functions disappear, and are replaced by purely arithmetical functions.

We have $\nu = P - 2\mu$, where μ is an integer prime to P and less than $\frac{1}{2}P$; moreover

$$(\nu \mid P) = (-2\mu \mid P) = -(2 \mid P)(\mu \mid P);$$

therefore
$$H = -\frac{\pi}{2P}(2 \mid P)\,\Sigma\,(\mu \mid P)\tan\frac{\mu\pi}{P}$$
$$= \frac{\pi i}{2P}(2 \mid P)\,\Sigma\,(\mu \mid P)\frac{r^\mu - 1}{r^\mu + 1},$$

where $r = e^{2\pi i/P}$, and the sum is taken for $\mu = 1, 2, 3 \dots \frac{1}{2}(P-1)$ with the convention that $(\mu \mid P) = 0$ when μ is not prime to P.

If we write $P - \mu$ for μ, the expression remains unaltered, so that

$$H = \frac{\pi i}{4P}(2 \mid P)\,\Sigma\,(\lambda \mid P)\frac{r^\lambda - 1}{r^\lambda + 1},$$
$$[\lambda = 1, 2, 3, \dots (P-1)].$$

Now if ω is any root of the equation $\omega^P - 1 = 0$,

$$\frac{\omega - 1}{\omega + 1} = \frac{\omega(1 - \omega^{P-1})}{1 + \omega}$$
$$= \omega - \omega^2 + \omega^3 - \dots - \omega^{P-1}$$
$$= \sum_1^{P-1}(-1)^{a-1}\omega^a;$$

hence
$$H = \frac{\pi i}{4P}(2 \mid P)\sum_{\lambda, a}(-1)^{a-1}(\lambda \mid P)\,r^{\lambda a}.$$

But by Art. 191

$$\sum_{\lambda} (\lambda \mid P)\, r^{\lambda\alpha} = (\alpha \mid P) \sum (\lambda \mid P)\, r^{\lambda}$$
$$= (\alpha \mid P)\, i\sqrt{P};$$

therefore $$H = \frac{\pi}{4\sqrt{P}} (2 \mid P) \sum_{1}^{P-1} (-1)^{\alpha} (\alpha \mid P).$$

This may be further simplified: for if α is even, we may put

$$\alpha = 2\alpha',$$

whence $$(2 \mid P)(-1)^{\alpha} (\alpha \mid P) = (\alpha' \mid P);$$

while if α is odd, we may put

$$\alpha = P - 2\alpha',$$

and then $$(2 \mid P)(-1)^{\alpha} (\alpha \mid P) = (\alpha' \mid P)$$

as before. The values of α' in each case are

$$1, 2, 3 \ldots \tfrac{1}{2}(P-1):$$

so that finally $$H = \frac{\pi}{2\sqrt{P}} \sum_{1}^{\frac{1}{2}(P-1)} (\alpha' \mid P).$$

The number of classes is therefore

$$h = \frac{2H\sqrt{P}}{\pi} = \Sigma (\alpha' \mid P):$$

or, in words;

When $D = -P \equiv 1 \pmod 4$, where P involves no square factor, the number of properly primitive classes for the determinant D is equal to the excess of the number of positive integers α', less than $\frac{1}{2}P$, for which $(\alpha' \mid P) = +1$ over the number of those for which $(\alpha' \mid P) = -1$; it being understood that $(\alpha' \mid P) = 0$ when α' is not prime to P.

When P is a prime of the form $4n + 3$, the number of properly primitive classes is simply the excess of the number of quadratic residues of P contained in the series

$$1, 2, 3 \ldots \tfrac{1}{2}(P-1)$$

above the number of non-residues.

For instance, if $P = 11$, the residues are 1, 3, 4, 5, while there is only one non-residue, namely 2; hence $h = 4 - 1 = 3$, which is right, the positive properly primitive classes being represented by (1, 0, 11), (3, ± 1, 4).

II. Let $$D = -P \equiv 3 \pmod 4).$$

In this case $(D \mid n) = (-1)^{\frac{1}{2}(n-1)} (n \mid P)$, so that

$$H = \Sigma \frac{(-1)^{\frac{1}{2}(n-1)}}{n} (n \mid P)$$

$$= \Sigma (-1)^{\frac{1}{2}(\nu-1)} (\nu \mid P) \left\{ \frac{1}{\nu} + \frac{1}{2P-\nu} - \frac{1}{2P+\nu} - \frac{1}{4P-\nu} + \frac{1}{4P+\nu} + \dots \right\}$$

$$= \frac{\pi}{2P} \Sigma (-1)^{\frac{1}{2}(\nu-1)} (\nu \mid P) \operatorname{cosec} \frac{\nu\pi}{2P}$$

$$= \frac{\pi}{2P} (2 \mid P) \Sigma (-1)^{\mu} (\mu \mid P) \sec \frac{\mu\pi}{P}.$$

Writing $\mu = 2\mu'$, or $\mu = P - 2\mu'$ according as μ is even or odd, this easily reduces to

$$\frac{\pi}{2P} \Sigma (\mu' \mid P) \sec \frac{2\mu'\pi}{P},$$

where μ', like μ, assumes the values 1, 2, 3.. $\frac{1}{2}(P-1)$.

Omitting the accent, and introducing r, we have

$$H = \frac{\pi}{2P} \Sigma (\mu \mid P) \sec \frac{2\mu\pi}{P}$$

$$= \frac{\pi}{4P} \Sigma (\lambda \mid P) \sec \frac{2\lambda\pi}{P}$$

$$= \frac{\pi}{2P} \sum_{1}^{P-1} (\lambda \mid P) \frac{r^{\lambda}}{1 + r^{2\lambda}}.$$

Now, if ω is any complex root of $\omega^P - 1 = 0$,

$$\frac{\omega}{1+\omega^2} = \frac{1}{\omega + \omega^{-1}}$$

$$= 1 + \omega^4 + \omega^{-4} + \omega^8 + \omega^{-8} + \dots + \omega^{P-1} + \omega^{-P+1};$$

therefore $$H = \frac{\pi}{2P} \sum_{\lambda, \alpha''} (\lambda \mid P) \{1 + r^{4\lambda\alpha''} + r^{-4\lambda\alpha''}\},$$

or since

$$\sum_{\lambda} (\lambda \mid P) = 0, \quad \sum_{\lambda} (\lambda \mid P) r^{4\lambda\alpha''} = \sum_{\lambda} (\lambda \mid P) r^{-4\lambda\alpha''} = (\alpha'' \mid P)\sqrt{P},$$

we have $$H = \frac{\pi}{\sqrt{P}} \Sigma (\alpha'' \mid P),$$

where the values of α'' are 1, 2, 3...$\frac{1}{4}(P-1)$.

Finally $$h = 2\Sigma (\alpha'' \mid P).$$

For example let $P = 77$. Here $(\alpha'' \mid P) = 0$ when $\alpha'' = 7, 11, 14$, $(\alpha'' \mid P) = 1$ when $\alpha'' = 1, 4, 6, 9, 10, 13, 15, 16, 17, 19$, while $(\alpha'' \mid P) = -1$ for the remaining six values of α''; hence

$$h = 2(10 - 6) = 8.$$

The representative forms for the determinant -77 are in fact $(1, 0, 77)$, $(7, 0, 11)$, $(2, 1, 39)$, $(9, 2, 9)$, $(3, \pm 1, 26)$, $(6, \pm 1, 13)$, eight in all.

III. Let $$D = -2P \equiv 2 \pmod 8.$$

Here $(D|n) = (-1)^{\frac{1}{8}(n^2-1)}(n|P)$, and

$$H = \Sigma \frac{(-1)^{\frac{1}{8}(n^2-1)}}{n}(n|P).$$

Observing that, if n is odd,

$$\begin{aligned}(4P \pm n)^2 - n^2 &= 16P^2 \pm 8Pn\\ &\equiv \pm 8 \pmod{16},\end{aligned}$$

we see that the expression H may be written in the form

$$\begin{aligned}H &= \Sigma(-1)^{\frac{1}{8}(\nu^2-1)}(\nu|P)\left\{\frac{1}{\nu} + \frac{1}{4P-\nu} - \frac{1}{4P+\nu} - \frac{1}{8P-\nu}\right.\\ &\qquad\left. + \frac{1}{8P+\nu} + \dots\right\}\\ &= \frac{\pi}{4P}\Sigma(-1)^{\frac{1}{8}(\nu^2-1)}(\nu|P)\operatorname{cosec}\frac{\nu\pi}{4P}\\ &\qquad [\nu = 1, 3, 5 \dots (2P-1)].\end{aligned}$$

By adding the first term to the last, the second to the last but one, and so on, this becomes

$$\begin{aligned}H = \frac{\pi\sqrt{2}}{2P}&\left\{\frac{\cos\frac{(P-1)\pi}{4P}}{\cos\frac{(P-1)\pi}{2P}} - (3|P)\frac{\sin\frac{(P-3)\pi}{4P}}{\cos\frac{(P-3)\pi}{2P}} - (5|P)\frac{\cos\frac{(P-5)\pi}{4P}}{\cos\frac{(P-5)\pi}{2P}}\right.\\ &\qquad\left. + (7|P)\frac{\sin\frac{(P-7)\pi}{4P}}{\cos\frac{(P-7)\pi}{2P}} + \dots\right\}.\end{aligned}$$

Now if $\frac{P+\nu}{4}$ is an integer, it is evident that

$$\left(\frac{P+\nu}{4}\middle|P\right) = (\nu|P):$$

also
$$\cos\frac{(P-\nu)\pi}{4P} = \sin\frac{(P+\nu)\pi}{4P},$$

$$\cos\frac{(P-\nu)\pi}{2P} = -\cos\frac{(P+\nu)\pi}{2P}:$$

hence the above expression may be written

$$H = \frac{\pi\sqrt{2}}{2P}\left\{ -\left(\frac{P+1}{4}\,\middle|\,P\right)\frac{\sin\dfrac{(P+1)\pi}{4P}}{\cos\dfrac{(P+1)\pi}{2P}} + \left(\frac{P-3}{4}\,\middle|\,P\right)\frac{\sin\dfrac{(P-3)\pi}{4P}}{\cos\dfrac{(P-3)\pi}{2P}} \right.$$

$$\left. + \left(\frac{P+5}{4}\,\middle|\,P\right)\frac{\sin\dfrac{(P+5)\pi}{4P}}{\cos\dfrac{(P+5)\pi}{2P}} - \dots \right\}.$$

The term $\dfrac{\sin\dfrac{\pi}{P}}{\cos\dfrac{2\pi}{P}}$ has a coefficient $+1$ or -1 according as $P \equiv 7$ or $3 \pmod 8$: hence we have, by rearranging the terms,

$$H = \frac{\pi\sqrt{2}}{2P}(2|P)\,\Sigma\,(-1)^{\mu-1}(\mu|P)\frac{\sin\dfrac{\mu\pi}{P}}{\cos\dfrac{2\mu\pi}{P}}$$

$$[\mu = 1, 2, 3 \dots \tfrac{1}{2}(P-1)].$$

If we change μ into $P-\mu$, $(-1)^{\mu-1}$ becomes $(-1)^{\mu}$, and $(\mu|P)$ becomes $-(\mu|P)$, while the trigonometrical factor is unaltered: hence

$$H = \frac{\pi\sqrt{2}}{4P}(2|P)\,\Sigma\,(-1)^{\lambda-1}(\lambda|P)\frac{\sin\dfrac{\lambda\pi}{P}}{\cos\dfrac{2\lambda\pi}{P}}$$

$$[\lambda = 1, 2, 3 \dots (P-1)].$$

Writing 2μ for the even values of λ, and $P-2\mu$ for the odd values, this becomes, after some easy reductions, similar to those employed in the previous cases,

$$H = -\frac{\pi\sqrt{2}}{2P}\,\Sigma\,(\mu|P)\frac{\sin\dfrac{2\mu\pi}{P}}{\cos\dfrac{4\mu\pi}{P}}$$

$$[\mu = 1, 2, 3 \dots \tfrac{1}{2}(P-1)].$$

If we write $P-\mu$ for μ, this expression is unaltered, so that finally

$$H = -\frac{\pi\sqrt{2}}{4P}\,\Sigma\,(\lambda|P)\frac{\sin\dfrac{2\lambda\pi}{P}}{\cos\dfrac{4\lambda\pi}{P}}$$

$$= \frac{i\pi\sqrt{2}}{4P}\,\Sigma\,(\lambda|P)\,\frac{r^{\lambda} - r^{-\lambda}}{r^{2\lambda} + r^{-2\lambda}},$$

where $r = e^{2\pi i/P}$, and the values of λ are $1, 2, 3 \ldots (P-1)$.

Now if ω is any complex root of the equation $\omega^P - 1 = 0$,

$$\frac{\omega - \omega^{-1}}{\omega^2 + \omega^{-2}} = -\,(\omega - \omega^{-1} - \omega^5 + \omega^{-5} + \omega^9 - \omega^{-9} - \ldots),$$

where the series ends with $\pm\,\omega^{P-2} \mp \omega^{-P+2}$. Hence

$$H = -\frac{i\pi\sqrt{2}}{4P}\,\Sigma\,(\lambda|P)\,\{r - r^{-1} - r^5 + r^{-5} + \ldots\}$$

$$= \frac{\pi}{\sqrt{2P}}\,\{1 - (5|P) + (9|P) - (13|P) + \ldots\},$$

where the series ends with $\pm\,(\overline{P-2}|P)$.

The value of h is therefore

$$h = 2\,\{1 - (5|P) + (9|P) - (13|P) + \ldots \pm (\overline{P-2}|P)\},$$

where it must be remembered that $(m|P)$ is to be put equal to zero when m is not prime to P.

For example let $D = -94 = -2\,.\,47$. We find from Gauss's table of quadratic characters that

$$1,\ \ 9,\ 17,\ 25\,R47,\quad 33,\ 41\,N47,$$
$$5,\ 13,\ 29,\ 45\,N47,\quad 21,\ 37\,R47,$$

hence $h = 2\,(8 - 4) = 8$.

Or again, if $D = -30 = -2\,.\,15$, we have

$$h = 2\,\{1 - (5|15) + (9|15) - (13|15)\}$$
$$= 2\,\{1 - 0 + 0 + 1\} = 4.$$

The expression for the class-number may be reduced to the form

$$h = 2\Sigma\,(\alpha|P),$$

where the summation applies to all integers α for which

$$\tfrac{1}{8}P < \alpha < \tfrac{3}{8}P.$$

For suppose $P \equiv 7 \pmod 8$: then $(2|P) = 1$, and the quadratic characters, with regard to P, of

$$1,\ -5,\ 9 \ldots (P-6),\ -(P-2)$$

will be the same as those of

$$\tfrac{1}{8}(P+1),\ \tfrac{1}{8}(3P-5),\ \tfrac{1}{8}(P+9), \ldots \tfrac{1}{8}(2P-6),\ \tfrac{1}{8}(2P+2).$$

Similarly when $P \equiv 3 \pmod 8$, the characters will be the same as those of

$$\tfrac{1}{8}(3P-1),\ \tfrac{1}{8}(P+5),\ \tfrac{1}{8}(3P-9)\ldots\tfrac{1}{8}(2P-6),\ \tfrac{1}{8}(2P+2),$$

and in each case it is easy to see that h may be expressed as above stated.

For instance, if $P = 23$,

$$\begin{aligned} h &= 2\{1-(5|23)+(9|23)-(13|23)+(17|23)-(21|23)\} \\ &= 2\{(3|23)+(8|23)+(4|23)+(7|23)+(5|23)+(6|23)\} \\ &= 2\Sigma(\alpha|P); \end{aligned}$$

and if $P = 11$,

$$\begin{aligned} h &= 2\{1-(5|11)+(9|11)\} \\ &= 2\{(4|11)+(2|11)+(3|11)\} \\ &= 2\Sigma(\alpha|P) \end{aligned}$$

as before.

IV. Let $D = -2P \equiv 6 \pmod 8$.

Proceeding as in last case, we find that

$$\begin{aligned} H &= \Sigma\,\frac{(-1)^{\frac{1}{8}(n^2-1)+\frac{1}{2}(n-1)}}{n}(n|P) \\ &= \frac{\pi}{4P}\Sigma(-1)^{\frac{1}{8}(\nu^2-1)+\frac{1}{2}(\nu-1)}(\nu|P)\operatorname{cosec}\frac{\nu\pi}{4P} \\ &\qquad\qquad [\nu = 1,\ 3,\ 5\ldots(2P-1)] \\ &= \frac{\pi\sqrt{2}}{2P}(2|P)\,\Sigma(-1)^{\mu}(\mu|P)\,\frac{\cos\frac{\mu\pi}{P}}{\cos\frac{2\mu\pi}{P}} \\ &\qquad\qquad [\mu = 1,\ 2,\ 3\ldots\tfrac{1}{2}(P-1)] \\ &= \frac{\pi\sqrt{2}}{4P}\Sigma(\lambda|P)\,\frac{\cos\frac{2\lambda\pi}{P}}{\cos\frac{4\lambda\pi}{P}} \\ &\qquad\qquad [\lambda = 1,\ 2,\ 3\ldots(P-1)] \\ &= \frac{\pi\sqrt{2}}{4P}\Sigma(\lambda|P)\,\frac{r^{\lambda}+r^{-\lambda}}{r^{2\lambda}+r^{-2\lambda}}. \end{aligned}$$

Now if ω is any complex root of $\omega^P - 1 = 0$,

$$\frac{\omega+\omega^{-1}}{\omega^2+\omega^{-2}} = \omega+\omega^{-1}-\omega^5-\omega^{-5}+\omega^9+\omega^{-9}-\ldots\pm(\omega^{P-4}+\omega^{-P+4})\mp 1.$$

Expanding $\frac{r^{\lambda} + r^{-\lambda}}{r^{2\lambda} + r^{-2\lambda}}$ by this formula, and remembering that $\Sigma (\lambda | P) = 0$, we obtain

$$H = \frac{\pi}{\sqrt{2P}} \{1 - (5|P) + (9|P) - \ldots \pm (\overline{P-4}|P)\},$$

and therefore $\qquad h = 2\{1 - (5|P) + (9|P) - \ldots\}.$

This is the same formula as in last case; the only difference is that the number of terms is $\frac{1}{4}(P-1)$ instead of $\frac{1}{4}(P+1)$.

By reasoning exactly similar to that employed for case III., the expression for h may be reduced to the form

$$h = 2\{\Sigma(\alpha|P) - \Sigma(\beta|P)\},$$

where the summations apply to all values of α and β such that

$$0 < \alpha < \tfrac{1}{8}P, \quad \tfrac{3}{8}P < \beta < \tfrac{1}{2}P.$$

It may be convenient to exhibit the results for a negative determinant in the following tabular form:

$$\text{I.} \quad D = -P \equiv 1 \pmod{4}, \qquad h = \overset{4}{\underset{0}{\Sigma}} (\alpha|P),$$

$$\text{II.} \quad D = -P \equiv 3 \pmod{4}, \qquad h = 2\overset{2}{\underset{0}{\Sigma}} (\alpha|P),$$

$$\text{III.} \quad D = -2P \equiv 2 \pmod{8}, \qquad h = 2\overset{3}{\underset{1}{\Sigma}} (\alpha|P),$$

$$\text{IV.} \quad D = -2P \equiv 6 \pmod{8}, \qquad h = 2\{\overset{1}{\underset{0}{\Sigma}} (\alpha|P) - \overset{4}{\underset{3}{\Sigma}} (\alpha|P)\}.$$

Here the symbol $\overset{q}{\underset{p}{\Sigma}} (\alpha|P)$ is used to express that the sum is to be taken for all integral values of α such that $\frac{pP}{8} < \alpha < \frac{qP}{8}$. (Cf. Dirichlet, *Zahlentheorie*, p. 275.)

207. The remaining four cases relate to a positive determinant.

V. Let $\qquad D = P \equiv 1 \pmod{4}.$

Here $\qquad H = \Sigma(D|n)\frac{1}{n} = \Sigma(n|P)\frac{1}{n}.$

Multiply both sides by

$$\sqrt{P} = \Sigma(\lambda|P) r^{\lambda}$$

$$[r = e^{2\pi i/P};\ \lambda = 1,\ 2,\ 3 \ldots (P-1)],$$

then, observing that $\Sigma(\lambda|P)\, r^{n\lambda} = (n|P)\,\Sigma(\lambda|P)\, r^{\lambda}$, we have

$$H\sqrt{P} = \Sigma(\lambda|P)\left\{r^{\lambda} + \frac{1}{3}r^{3\lambda} + \frac{1}{5}r^{5\lambda} + \ldots\right\}.$$

Now if $x = \rho e^{\theta i}$, when ρ is positive and less than 1,

$$x + \frac{1}{3}x^3 + \frac{1}{5}x^5 + \ldots = \frac{1}{2}\log\frac{1+x}{1-x}$$

$$= \frac{1}{4}\log\frac{1 + 2\rho\cos\theta + \rho^2}{1 - 2\rho\cos\theta + \rho^2} + i\tan^{-1}\frac{2\rho\sin\theta}{1-\rho^2};$$

and the limit of the real part of this when $\rho = 1$ is

$$\frac{1}{4}\log\frac{1+\cos\theta}{1-\cos\theta} = \frac{1}{4}\log\cot^2\frac{\theta}{2} = \frac{1}{2}\log\left|\cot\frac{\theta}{2}\right|.$$

Since $H\sqrt{P}$ is real, it is unnecessary to consider the limiting value of the imaginary part, and we have

$$H = \frac{1}{2\sqrt{P}}\,\Sigma(\lambda|P)\log\left|\cot\frac{\lambda\pi}{P}\right|.$$

Consequently

$$h\log(T + U\sqrt{D}) = 2H\sqrt{P} = \Sigma(\lambda|P)\log\left|\cot\frac{\lambda\pi}{P}\right|$$

$$= \log\frac{\Pi\left|\cot\frac{\alpha\pi}{P}\right|}{\Pi\left|\cot\frac{\beta\pi}{P}\right|},$$

where the product applies to all values of α between 0 and P for which $(\alpha|P) = 1$, and to all values of β between 0 and P for which $(\beta|P) = -1$.

If we write $\alpha = P - \alpha'$, and $\beta = P - \beta'$, when α or β exceeds $\frac{1}{2}P$, the formula is reduced to

$$h\log(T + U\sqrt{D}) = 2\log\frac{\Pi\cot\frac{a\pi}{P}}{\Pi\cot\frac{b\pi}{P}},$$

with the conditions

$$0 < a < \tfrac{1}{2}P,\ \ (a|P) = 1;\quad 0 < b < \tfrac{1}{2}P,\ \ (b|P) = -1.$$

For instance, if $P = 5$, then $a = 1$, $b = 2$, and

$$\frac{\cot\frac{\pi}{5}}{\cot\frac{2\pi}{5}} = 2 + \sqrt{5},\quad T + U\sqrt{5} = 9 + 4\sqrt{5},$$

and therefore $\qquad h = 1.$

VI. $$D = P \equiv 3 \pmod{4}.$$

Here $$H = \Sigma\,(-1)^{\frac{1}{2}(n-1)}\,(n|P)\,\frac{1}{n},$$

$$i\sqrt{P} = \Sigma\,(\lambda|P)\,r^{\lambda},$$

$$iH\sqrt{P} = \Sigma\,(\lambda|P)\left\{r^{\lambda} - \frac{1}{3}\,r^{3\lambda} + \frac{1}{5}\,r^{5\lambda} - \dots\right\},$$

and $H\sqrt{P}$ is equal to the real part of

$$-\Sigma\,(\lambda|P)\left\{x + \frac{1}{3}\,x^{3} + \frac{1}{5}\,x^{5} + \dots\right\},$$

where $$x = ir^{\lambda} = e^{\left(\frac{\pi}{2} + \frac{2\lambda\pi}{P}\right)i}.$$

As before, this is

$$-\Sigma\,(\lambda|P)\log\left|\cot\left(\frac{\pi}{4} + \frac{\lambda\pi}{P}\right)\right|;$$

and therefore, with the same notation as before,

$$h\log(T + U\sqrt{D}) = \log\frac{\Pi\left|\tan\left(\frac{\pi}{4} + \frac{\alpha\pi}{P}\right)\right|}{\Pi\left|\tan\left(\frac{\pi}{4} + \frac{\beta\pi}{P}\right)\right|}.$$

This may be written in a somewhat simpler form if we observe that the series of numbers $P + 4\alpha$ are congruent (mod $4P$) to all the integers m between 0 and $4P$ which satisfy the conditions $m \equiv 3 \pmod{4}$, $(m|P) = 1$; while the integers $-P + 4\beta$ are congruent (mod $4P$) to all the integers n between 0 and $4P$ which satisfy the conditions $n \equiv 1 \pmod{4}$, $(n\ P) = -1$. Hence if b stands for any one of the odd integers between 0 and $4P$ for which $(P|b) = -1$, this will comprise all the numbers m and n, so that

$$\frac{\Pi\left|\tan\left(\frac{\pi}{4} + \frac{\alpha\pi}{P}\right)\right|}{\Pi\left|\tan\left(\frac{\pi}{4} + \frac{\beta\pi}{P}\right)\right|} = \Pi\left|\tan\frac{(4\alpha + P)\,\pi}{4P}\right|.\,\Pi\left|\tan\frac{(4\beta - P)\,\pi}{4P}\right|$$

$$= \Pi\left|\tan\frac{b\pi}{4P}\right|.$$

Hence $$h\log(T + U\sqrt{D}) = \log\Pi\left|\tan\frac{b\pi}{4P}\right|.$$

Thus when $P = 3$, the values of b are 5 and 7; whence

$$\Pi\tan\frac{b\pi}{4P} = \tan\frac{5\pi}{12}\tan\frac{7\pi}{12} = -(2 + \sqrt{3})^{2} = -(T + U\sqrt{3})^{2},$$

so that $$h = 2.$$

VII. $$D = 2P \equiv 2 \pmod 8.$$

In this case $$H = \Sigma\,(-1)^{\frac{1}{8}(n^2-1)}\,(n|P)\,\frac{1}{n}.$$

$$\sqrt{P} = \Sigma\,(\lambda|P)\,r^{\lambda},$$

and therefore

$$H\sqrt{P} = \Sigma\,(\lambda|P)\left\{r^{\lambda} - \frac{1}{3}\,r^{3\lambda} - \frac{1}{5}\,r^{5\lambda} + \frac{1}{7}\,r^{7\lambda} + \ldots\right\}.$$

Now it is easily proved that if

$$\theta = \frac{1+i}{\sqrt{2}} = e^{\pi i/4},$$

and $|x| < 1$,

$$x - \frac{1}{3}\,x^3 - \frac{1}{5}\,x^5 + \frac{1}{7}\,x^7 - \ldots = \frac{1}{2\sqrt{2}}\log\frac{(1+\theta x)(1+\theta^{-1}x)}{(1-\theta x)(1-\theta^{-1}x)}.$$

Putting $x = r^{\lambda}$, and attending only to the real part of the logarithm, we find that

$$H = \frac{1}{2\sqrt{2P}}\,\Sigma\,(\lambda|P)\log\left|\cot\left(\frac{\lambda\pi}{P} + \frac{\pi}{8}\right)\cot\left(\frac{\lambda\pi}{P} - \frac{\pi}{8}\right)\right|,$$

and consequently

$$h\log(T + U\sqrt{D}) = \log\frac{\Pi\left|\cot\left(\frac{\alpha\pi}{P} + \frac{\pi}{8}\right)\cot\left(\frac{\alpha\pi}{P} - \frac{\pi}{8}\right)\right|}{\Pi\left|\cot\left(\frac{\beta\pi}{P} + \frac{\pi}{8}\right)\cot\left(\frac{\beta\pi}{P} - \frac{\pi}{8}\right)\right|}.$$

This may be reduced to the form

$$h\log(T + U\sqrt{D}) = \log\Pi\left|\tan\frac{b\pi}{8P}\right|,$$

with the conditions

$$0 < b < 8P, \qquad (2P|b) = -1.$$

Thus if $P = 5$, the values of b are 7, 11, 17, 19, 21, 23, 29, 33; and hence

$$h\log(T + U\sqrt{D}) = \log\left(\tan^2\frac{7\pi}{40}\tan^2\frac{11\pi}{40}\tan^2\frac{19\pi}{40}\tan^2\frac{21\pi}{40}\right)$$

$$= \log(19 + 6\sqrt{10})^2,$$

and therefore $$h = 2.$$

It may be observed that $4P - b$ is congruent (mod $8P$) to a number a such that

$$0 < a < 8P, \qquad (2P|a) = 1,$$

hence $$\cos\frac{b\pi}{8P}=\sin\frac{a\pi}{8P}\text{; and we may write}$$

$$h\log(T+U\sqrt{D})=\log\frac{\Pi\sin\dfrac{b\pi}{8P}}{\Pi\sin\dfrac{a\pi}{8P}}$$

$$[0<a<8P,\quad (2P|a)=1;\qquad 0<b<8P,\quad (2P|b)=-1].$$

The formula is not applicable when $D=2$: it is easily found that in this case $h=1$.

VIII. $D=2P\equiv 6 \pmod 8$.

The work is so much like that of the last case that it is needless to give it in detail. The result is that, with the same notation as in the last case,

$$h\log(T+U\sqrt{D})=\log\frac{\Pi\left|\cot\left(\dfrac{\alpha\pi}{P}-\dfrac{\pi}{8}\right)\tan\left(\dfrac{\alpha\pi}{P}+\dfrac{\pi}{8}\right)\right|}{\Pi\left|\cot\left(\dfrac{\beta\pi}{P}-\dfrac{\pi}{8}\right)\tan\left(\dfrac{\beta\pi}{P}+\dfrac{\pi}{8}\right)\right|}$$

$$=\log\Pi\left|\tan\frac{b\pi}{8P}\right|$$

$$=\log\frac{\Pi\sin\dfrac{b\pi}{8P}}{\Pi\sin\dfrac{a\pi}{8P}}.$$

For example when $D=6$, the values of b are 7, 11, 13, 17, so that

$$\Pi\tan\frac{b\pi}{8P}=\tan^2\frac{7\pi}{24}\tan^2\frac{11\pi}{24}=(5+2\sqrt{6})^2,$$

and hence $$h=2.$$

Many other forms may be given to the expression for h; those which have been found above appear to be the simplest. It will be convenient to collect them in the following tabular form.

$$D\equiv 1 \pmod 4),$$

$$h\log(T+U\sqrt{D})=\log\frac{\Pi\left|\tan\dfrac{b\pi}{D}\right|}{\Pi\left|\tan\dfrac{a\pi}{D}\right|}$$

$$[0<a<D,\quad (a|D)=1;\qquad 0<b<D,\quad (b|D)=-1].$$

$$D \not\equiv 1 \pmod 4,$$

$$h \log (T + U\sqrt{D}) = \log \Pi \left| \tan \frac{b\pi}{4D} \right|$$

$$= \log \frac{\Pi \sin \dfrac{b\pi}{4D}}{\Pi \sin \dfrac{a\pi}{4D}},$$

where a, b denote odd integers such that

$$0 < a < 4D, \quad (D|a) = 1; \qquad 0 < b < 4D, \quad (D|b) = -1.$$

208. The method of last article may also be applied when D is negative. The work is much the same, except that in the logarithms which occur, it is the imaginary parts which have to be retained, and since these are many-valued, some care is necessary to ensure the correct values being taken.

For a discussion of this point, and for a somewhat different way of effecting the summation, the reader is referred to Dirichlet (*Recherches*, etc. § 10, or *Zahlentheorie*, §§ 102—6) and Smith (*Report*, Art. 104). It may be added that the value of h, obtained in this way, presents itself in a form different to that given above; but there is no difficulty in showing that the results of the two methods are in agreement.

209. There are many reasons in favour of adopting as the typical expression for a primitive quadratic form

$$ax^2 + bxy + cy^2$$

with a determinant $\qquad D = b^2 - 4ac,$

where a, b, c are integers without any common divisor except unity.

It is clear that

$$D \equiv 0 \text{ or } 1 \pmod 4,$$

and that, conversely, if D satisfies one of these conditions, there will be primitive forms of determinant D.

We may put $\qquad D = D_0 Q^2,$

where $D_0 \equiv 0$ or $1 \pmod 4$, and D_0 involves no square factor, except when $D_0 \equiv 0 \pmod 4$, and $\frac{1}{4}D_0$ is of the form $4k+2$ or $4k+3$, in which case the square factor 4, but no other, is retained in D_0. Thus D_0 satisfies one or other of the conditions

$$D_0 = P, \quad P \equiv 1 \pmod 4,$$
$$D_0 = 4P, \quad P \equiv -1 \pmod 4,$$
$$D_0 = 8P, \quad P \equiv \pm 1 \pmod 4,$$

where P involves no square factor. Numbers such as D_0 may be called (after Kronecker) *fundamental* discriminants. This being so, the number of classes of primitive forms for a fundamental discriminant D_0 may be expressed by the following formulae.

I. $$D_0 < 0,$$

$$h = \frac{\tau}{D_0} \Sigma (D_0|k) k \quad [k = 1, 2, 3, \ldots (-D_0 - 1)],$$

where $\tau = 3$ for $D_0 = -3$, $\tau = 2$ for $D_0 = -4$, $\tau = 1$ for $D_0 < -4$.

II. $$D_0 > 0,$$

$$h \log E(D_0) = -\Sigma (D_0|k) \log (1 - e^{2k\pi i/D_0})$$
$$[k = 1, 2, 3 \ldots (D_0 - 1)],$$

where $E(D_0)$ denotes $\frac{1}{2}(T + U\sqrt{D_0})$, T, U being the least positive integers such that $T^2 - D_0 U^2 = 4$.

It is to be remembered that $(D_0|k)$ is to be put equal to zero when k is not prime to D_0.

As in Arts. 150, 151, it may be proved that if

$$D' = D_0 Q^2,$$

where D_0 is a fundamental discriminant, the number of primitive classes for the determinant D' is

$$h' = hQ \frac{\log E(D_0)}{\log E(D)} \Pi \left\{1 - \frac{1}{q}(D_0|q)\right\},$$

where h is the number of primitive classes for the determinant D_0, and the product applies to all prime factors of Q which do not divide D_0.

These results are taken from Kronecker's researches on elliptic functions (*Zur Theorie der elliptischen Functionen*, Berlin Sitzungsberichte for April, 1885, p. 768). It is easy enough to prove that they are in agreement with the ordinary theory; the simplification which is gained is obvious. It may be specially noticed that in the modified theory improperly primitive forms do not occur.

The discussion of Kronecker's very important memoirs must be, for the present, postponed; and in the rest of this chapter only quadratic forms of the ordinary type will be considered.

210. It is unnecessary to enlarge upon the very remarkable character of the foregoing investigation, whether it be regarded as the direct determination of the class-number, or as the expression, in terms of the class-number, of the sums of certain infinite series. There are, however, two points which deserve to be emphasized. The first of these relates to the distribution of the residues and non-residues of a given number. For simplicity take the case of a prime negative determinant $D=-p$, where p is a prime of the form $4n+3$. The formula (p. 247)

$$h = \sum_{0}^{4} (\alpha \mid p),$$

combined with the remark that h is necessarily a *positive* integer, leads to the conclusion that in the series

$$1,\ 2,\ 3 \ldots \tfrac{1}{2}(p-1),$$

there are more quadratic residues of p than non-residues. It does not appear that any independent proof of this proposition has ever been discovered. If any such proof could be found, it is not impossible that it might lead to a determination of h without the use of infinite series. Similar remarks apply to the other formulæ for negative determinants.

The other point to be noticed is that when D is positive we are able to construct a solution of the Pellian equation by means of trigonometrical formulæ; the solution thus obtained being not the fundamental solution, but one of which the place in the series of solutions depends upon the value of h. Dirichlet has verified *a posteriori* that the trigonometrical expressions which occur in the determination of h do in fact lead to integral solutions of the Pellian equation. For the complete discussion the reader is referred to his memoir (*Sur la manière de résoudre l'équation $t^2 - pu^2 = 1$ au moyen des fonctions circulaires*, Crelle, XVII. (1837), p. 286); it will be sufficient to consider here, by way of illustration, the case when $D=p$, a prime of the form $4n+1$, so that

$$h \log (T + U\sqrt{p}) = \log \frac{\Pi \left| \tan \dfrac{b\pi}{p} \right|}{\Pi \left| \tan \dfrac{a\pi}{p} \right|}.$$

With the notation of Chap. VII., we have

$$4\,\frac{x^p - 1}{x - 1} = Y^2 - pZ^2,$$

$$Y + Z\sqrt{p} = 2\Pi\,(x - r^a), \quad Y - Z\sqrt{p} = 2\Pi\,(x - r^b),$$

where

$$r = e^{2\pi i/p}.$$

Let f, g be the numerical values of Y, Z when $x=1$: then

$$f^2-pg^2=4p.$$

Hence f is a multiple of p, and if we put

$$f=pg', \qquad g=f',$$

then f', g' will be integers, and

$$f'^2-pg'^2=-4.$$

Similarly, if f'', g'' are the values of Y and Z when $x=-1$,

$$f''^2-pg''^2=4.$$

Hence

$$-\frac{f'-g'\sqrt{p}}{f'+g'\sqrt{p}}\cdot\frac{f''+g''\sqrt{p}}{f''-g''\sqrt{p}}=\frac{\Pi\,(1-r^b)\,\Pi\,(1+r^a)}{\Pi\,(1-r^a)\,\Pi\,(1+r^b)};$$

that is,
$$\frac{\Pi\tan\dfrac{b\pi}{p}}{\Pi\tan\dfrac{a\pi}{p}}=\frac{1}{16}(f'-g'\sqrt{p})^2(f''+g''\sqrt{p})^2$$

$$=\left(\frac{f'f''-pg'g''}{4}+\frac{f'g''-f''g'}{4}\sqrt{p}\right)^2.$$

Now if $p\equiv 1 \pmod 8$ it is easily seen that f', g', f'', g'' are all even; for if we suppose g' to be odd, $g'^2\equiv 1 \pmod 8$, and

$$f'^2=pg'^2-4\equiv 5 \pmod 8$$

which is impossible; and similarly for f'', g''. Hence $f'f''-pg'g''$ and $f'g''-f''g'$ are both multiples of 4, and

$$\frac{\Pi\tan\dfrac{b\pi}{p}}{\Pi\tan\dfrac{a\pi}{p}}=(t'+u'\sqrt{p})^2,$$

where (t', u') is an integral solution of $t'^2-pu'^2=-1$.

Consequently $\qquad (t'+u'\sqrt{p})^2=t+u\sqrt{p},$

where (t, u) is an integral solution of $t^2-pu^2=1$.

Next suppose $p\equiv 5 \pmod 8$. Then from the equations

$$\sqrt{p}\,(f'+g'\sqrt{p})=2\Pi\,(1-r^a),$$
$$(f''+g''\sqrt{p})=2\Pi\,(1+r^a),$$

it follows that

$$\sqrt{p}\,(f'+g'\sqrt{p})\,(f''+g''\sqrt{p})=4\Pi\,(1-r^{2a})$$
$$=2\Pi\,(1-r^b),$$

since $(2|p)=-1$; therefore

$$\sqrt{p}\,(f'+g'\sqrt{p})\,(f''+g''\sqrt{p})=2\sqrt{p}\,(f'-g'\sqrt{p}),$$

and hence

$$-2\,(f''+g''\sqrt{p})=(f'-g'\sqrt{p})^2,$$

$$\frac{(f'-g'\sqrt{p})^2\,(f''+g''\sqrt{p})^2}{16}=-\left(\frac{f''+g''\sqrt{p}}{2}\right)^3.$$

It may easily be shown that whether f'', g'' are both even or both odd,

$$\left(\frac{f''+g''\sqrt{p}}{2}\right)^3=t+u\sqrt{p},$$

where (t, u) is an integral solution of $t^2-pu^2=1$. This is obvious when f'', g'' are both even: if they are both odd, it follows from the fact that, to modulus 8,

$$f''\,(f''^2+3pg''^2)\equiv f''\,(1+3\,.\,5\,.\,1)\equiv 0,$$

and similarly

$$g''\,(pg''^2+3f''^2)\equiv g''\,(5\,.\,1+3\,.\,1)\equiv 0.$$

It is evident that f'', g'' cannot be one even and the other odd; hence in every case when $p\equiv 1 \pmod 4$

$$\frac{\Pi\tan\dfrac{b\pi}{p}}{\Pi\tan\dfrac{a\pi}{p}}=t+u\sqrt{p},$$

where (t, u) is an integral solution of $t^2-pu^2=1$.

It may be observed that when $p\equiv 1 \pmod 8$, $f''=2$ and $g''=0$; consequently $Y-2$ and Z involve the factor $x+1$. For instance, when $p=17$,

$$\begin{aligned} Y-2&=x\,(x+1)\,(2x^6-x^5+6x^4+x^3+3x^2+4x+1)\\ &=x\,(x+1)\,(x^3+2x+1)\,(2x^3-x^2+2x+1),\\ Z&=x\,(x+1)\,(x^2+1)\,(x^3+1).\end{aligned}$$

It may also be noticed that it follows from the foregoing analysis that when $p\equiv 5 \pmod 8$, and the equation $t^2-pu^2=4$ does not admit of odd solutions, the class-number is divisible by 3. This agrees with the results of Art. 153.

CHAPTER IX.

Applications of the Theory of Quadratic Forms.

211. In order to acquire complete familiarity with the theory of quadratic forms, it is indispensable to work out a considerable number of special cases. The student should have no difficulty in doing this, with the help of the examples which have been already given; and he cannot do better than draw up a complete classification for a series of positive and negative determinants, afterwards comparing his results with the tables of Gauss or Cayley. It is not easy to construct a large variety of exercises distinct from these direct applications: in fact, in the present state of the theory, every problem of a distinctly new type is apt to present unexpected difficulties, and its solution often requires the invention of new methods, and even of new principles. There are, however, a few problems of great interest to which the theory of quadratic forms has been successfully applied, and some of these will now be considered.

212. The first is the discovery of all the integral solutions, if any exist, of the general indeterminate equation

$$\phi = ax^2 + 2hxy + by^2 + 2gx + 2fy + c = 0.$$

Following the notation usually employed in analytical geometry, we shall write

$$\Delta = \begin{vmatrix} a & h & g \\ h & b & f \\ g & f & c \end{vmatrix},$$

$$A = bc - f^2, \quad B = ca - g^2, \quad C = ab - h^2,$$

$$F = gh - af, \quad G = hf - bg, \quad H = fg - ch.$$

Suppose, first, that neither b nor C is zero, and that C is not a negative square. Then the proposed equation may be multiplied by bC, and the result written in the form

$$(Cx-G)^2+C(hx+by+f)^2=-b\Delta.$$

If we put

$$\left.\begin{aligned} Cx-G&=X\\ hx+by+f&=Y\end{aligned}\right\}\text{.........................}(1),$$

then whenever (x, y) is an integral solution of $\phi=0$, (X, Y) is an integral solution of

$$X^2+CY^2=-b\Delta\text{.......................}(2),$$

and conversely, if (X, Y) is an integral solution of this equation,

$$\left.\begin{aligned} x&=\frac{X+G}{C}\\ y&=\frac{CY-hX+bF}{bC}\end{aligned}\right\}\text{.....................}(3),$$

gives a solution of $\phi=0$, provided these values of x and y are integral.

If C and $b\Delta$ are both positive, there are no real solutions of (2), and the proposed equation is insoluble. If C is positive and $b\Delta$ negative, there will be only a limited number of integral solutions of (2), if, indeed, there are any: so that it may be discovered by a finite number of trials whether there are any integral values of x and y.

If, on the other hand, C is negative, and (X_0, Y_0) is any integral solution of (2), there will be associated with this an infinite number of solutions, expressed by the formulae

$$\left.\begin{aligned} \pm X&=tX_0-uCY_0\\ \pm Y&=tY_0+uX_0\end{aligned}\right\}\text{.....................}(4),$$

where (t, u) is any integral solution of $t^2+Cu^2=1$, with t positive, and the ambiguities are independent.

If the upper sign is taken in each ambiguity, the corresponding values of x, y are

$$x=\frac{tX_0-uCY_0+G}{C},$$

$$y=\frac{t(CY_0-hX_0)+uC(X_0+hY_0)+bF}{bC}.$$

With respect to the modulus bC, the residues of the values (T_n, U_n) which satisfy the equation $T_n^2 + CU_n^2 = 1$ form a recurring series (see Art. 87); the same will therefore be true of the residues of the numerators of the expressions for x and y. Consequently, a limited number of trials will determine whether any of the values of x and y are integral. The process of trial has to be applied separately to each case arising from (4) by variation of sign in the ambiguities.

By way of illustration, take Gauss's example

$$x^2 + 8xy + y^2 + 2x - 4y + 1 = 0.$$

Here $\Delta = -36$, $C = -15$; and it is easily seen that all the integral solutions of

$$X^2 - 15Y^2 = 36$$

are given by $$\pm X = 6t, \quad \pm Y = 6u,$$
where (t, u) is any positive solution of $t^2 - 15u^2 = 1$.

We have $T_1 = 4$, $U_1 = 1$, and the series of residues of (T_n, U_n) to modulus 15 is (4, 1), (1, 0).

The general values of x, y are by (3)

$$\text{(i)} \quad x = \tfrac{1}{5}(2t + 3), \qquad y = -\tfrac{2}{5}(4t \pm 15u + 1);$$

$$\text{(ii)} \quad x = -\tfrac{1}{5}(2t - 3), \quad y = \tfrac{2}{5}(4t \pm 15u - 1);$$

and these are integral if we suppose that t is chosen in (i) so that $t \equiv 1 \pmod{15}$, and in (ii) so that $t \equiv 4 \pmod{15}$. For instance $t = 1$, $u = 0$ gives $x = 1$, $y = -2$; and $t = 4$, $u = 1$ leads to $x = -1$, $y = 0$ or 12.

If b happens to be zero, the equation $\phi = 0$ may be multiplied by aC, and the work proceeds as in the former case.

If a, b are both zero, and h is not zero, the equation may be written

$$(hx + f)(hy + g) = fg - \frac{ch}{2};$$

hence ch must be even, and if this condition is satisfied, then putting $fg - \frac{1}{2}ch = m$, we break up m into the product of two factors α, β in all possible ways, and find by trial all the integral solutions (if any) of

$$hx + f = \alpha, \quad hy + g = \beta$$

and $$hx + f = \beta, \quad hy + g = \alpha.$$

where $$\alpha\beta = m.$$

Returning to the general case, suppose $C=-m^2$, a negative square: then supposing b is not zero, the equation in X, Y is

$$(X+mY)(X-mY)=-b\Delta;$$

and this is solved by putting

$$X+mY=\alpha, \quad X-mY=\beta,$$

where $\alpha\beta=-b\Delta$, and examining all the different cases to see whether integral values of X and Y can be found. If this is the case, the corresponding values of x and y have to be examined. A particular case of C being a negative square is when a or b is zero, or again when a and b both vanish: these cases have been already considered.

Suppose, now, that $C=0$: then

$$ax^2+2hxy+by^2=m(\alpha x+\beta y)^2$$

where m, α, β are integers; and if we put

$$\alpha x+\beta y=z,$$

we have
$$mz^2+2gx+2fy+c=0;$$

and hence
$$m\beta z^2+2g\beta x+2f(z-\alpha x)+c\beta=0$$

or
$$x=\frac{m\beta z^2+2fz+c\beta}{2(f\alpha-g\beta)}.$$

The solutions, if any exist, of the congruence

$$m\beta z^2+2fz+c\beta\equiv 0 \ [\text{mod } 2(f\alpha-g\beta)]$$

will make x integral; and then these solutions must be examined separately to see whether the corresponding values of y are integral.

Here, again, there are various special cases which may occur: it is not worth while to discuss them in detail, but the following example may serve to illustrate the general method.

Let the equation be

$$3x^2+12xy+12y^2+4x-2y-85=0.$$

Putting $x+2y=z$, we find that

$$3z^2+5x-z-85=0;$$

hence we must have $3z^2-z\equiv 0 \pmod 5$,

leading to $z=5t$ or $5t+2$.

First, suppose $z=5t$; then

$$x=-15t^2+t+17$$
$$2y=15t^2+4t-17\equiv t^2-1 \pmod 2,$$

therefore t must be odd: let $t = 2u - 1$, then

$$x = -60u^2 + 62u + 1$$
$$y = 30u^2 - 26u - 3,$$

where u may be any integer.

If $$z = 5t + 2, \text{ then}$$
$$x = -15t^2 - 11t + 15$$
$$xy = 15t^2 + 16t - 13$$

and here again t must be odd; so that putting $t = 2u - 1$, we obtain the second set of solutions

$$x = -60u^2 + 38u + 11$$
$$y = 30u^2 - 14u - 7.$$

If, in the general case, $\Delta = 0$, the equation $\phi = 0$ assumes the form

$$(\alpha x + \beta y + \gamma)(\alpha' x + \beta' y + \gamma') = 0,$$

and its solutions are found by solving separately the linear indeterminate equations

$$\alpha x + \beta y + \gamma = 0, \quad \alpha' x + \beta' y + \gamma' = 0.$$

It is hardly necessary to add that if a, h, b all vanish the equation $\phi = 0$ is not of the second degree.

213. Another problem to which the theory of quadratic forms may be applied is that of finding out whether a given number is prime or composite. Theoretically the question may be answered by trying whether the number is divisible by any integer less than its square root; but when the given number is very large this method becomes impracticable.

The principle of the method which we are about to explain consists in discovering by trial a quadratic form by means of which the given number m, or any multiple of m, may be represented; the determinant of this form is a quadratic residue of m (Art. 59), and therefore of every prime factor of m. All possible factors of m must therefore belong to a certain set of linear forms (Art. 46), and it is therefore unnecessary to try any divisors not contained in the set. If another quadratic form, with a different determinant, can be found, by which m, or a multiple thereof, can be represented, the number of trial divisors may be still further reduced; and by proceeding in this way we may at last reduce the trial divisors to a sufficiently small set.

Before going into the general theory, it is advisable to give an example. Let $m = 173279$; then it will be found that

$$2m = 589^2 - 3 \,.\, 11^2.$$

Hence 3 is a quadratic residue of m, and therefore every prime divisor of m must be of the form $12n + 1$ or $12n + 11$. Moreover $\sqrt{m} < 417$, and the only numbers below this limit, comprised in the above linear forms, and exclusive of those which are obviously composite, are

$$\begin{array}{l} 13,\ 23,\ 37,\ 47,\ 59,\ 61,\ 71,\ 73,\ 83,\ 97 \\ 107,\ 109,\ 131,\ 133,\ 157,\ 167,\ 179,\ 181,\ 191,\ 193 \\ 227,\ 229,\ 239,\ 241,\ 251,\ 263,\ 277,\ 311,\ 313,\ 323 \\ 337,\ 349,\ 359,\ 373,\ 383,\ 397. \end{array}$$

If these divisors are tried successively it will be found that 241 is a factor of m: in fact

$$173279 = 241 \,.\, 719.$$

Since there are 78 odd primes less than 417, the number of trial divisors is, by this method, reduced by more than one-half.

It happens, in this case, that the resolution may be effected much more easily by observing that

$$3m = 721^2 - 4 = 723 \,.\, 719 = 3 \,.\, 241 \,.\, 719,$$

whence $m = 241 \,.\, 719$ as before. It will often be found that the methodical application of the process leads to the required resolution into factors in some such simple way as this: the advantage of the general theory is that each trial gives some information as to the character of the factors, and thus reduces the number of trial divisors.

In general, if we can express any multiple of m in the form

$$km = ax^2 + by^2,$$

where it may be supposed that a and b are free from square factors, and x, y are integers, one or both of which may be unity, it follows that

$$-abx^2 \equiv b^2y^2 \pmod{m},$$

and hence that $-ab$ is a quadratic residue of every prime factor of m. By means of decompositions of this kind, taken separately or in combination, it is usually not difficult to find a number of small quadratic residues of m; each of these imposes certain conditions upon the linear forms of the divisors of m, and the number of trial divisors is correspondingly reduced.

Suppose that, by any method, we have discovered a number D which is a quadratic residue of the odd number m; then the number of the solutions of the congruence

$$x^2 \equiv D \pmod{m},$$

is equal to 2^μ where μ is the number of different prime factors of μ (see Art. 35).

The congruence may be solved by the method of exclusion explained in Art. 47, and then from the number of solutions we may at once infer the number of different prime factors of m. Moreover if $x \equiv x_1$ and $x \equiv x_2$ are two solutions, we have

$$x_1^2 - x_2^2 = (x_1 + x_2)(x_1 - x_2) \equiv 0 \pmod{m},$$

so that if $x_1 + x_2$ is not a multiple of m, it must involve a factor of m, and this can be discovered by finding the greatest common divisor of m and $(x_1 + x_2)$. Thus the method not only enables us to decide whether m is prime or composite, but helps us to find the factors of m when it is not prime. It should be observed, however, that when m is a power of a single prime, we are unable in this way to detect the composite character of m.

Instead of solving the congruence $x^2 \equiv D \pmod{m}$, it is usually more convenient, to find by trial all the representations, or at least all the groups of representations of m by reduced forms of determinant D. Supposing that D is negative, say $D = -\Delta$, there will, in general, only be two representations (x, y), $(-x, -y)$ in each group; and it is obviously advantageous to choose, if possible, a value of Δ such that there are only a few classes in each genus. The particular genus which has to be considered can be found at once by determining the generic character of m.

If possible, a value of Δ should be chosen for which there is only one class in each genus. Of such determinants sixty-five are known, and are given in the following table; the Roman numeral prefixed to each group denotes the number of genera.

I. **1, 2, 3, 4, 7.**

II. **5, 6, 8, 9, 10, 12, 13, 15, 16, 18, 22, 25, 28, 37, 58.**

IV. **21, 24, 30, 33, 40, 42, 45, 48, 57, 60, 70, 72, 78, 85, 88, 93, 102, 112, 130, 133, 177, 190, 232, 253.**

VIII. **105, 120, 165, 168, 210, 240, 273, 280, 312, 330, 345, 357, 385, 408, 462, 520, 760.**

XVI. **840, 1320, 1365, 1848.**

It is highly probable, but has not been proved, that there are no other values of Δ which satisfy the condition in question.

214. Gauss has explained (*D. A.* Arts. 323—6) a tentative method for finding all the integral solutions, if any exist, of the equation

$$ax^2+by^2=m,$$

in which a, b, m denote given positive integers, without any common divisor except unity.

Let p be any prime which does not divide a, and let p^ν be the highest power of p which divides b. Take any power of p, say p^μ, and let n_1, n_2, n_3, etc. be the quadratic non-residues of p^μ.

Let the solutions of the linear congruences

$$az+bn_1\equiv m,\quad az+bn_2\equiv m,\quad az+bn_3\equiv m, \text{ etc. } (\text{mod } p^{\mu+\nu}),$$

be

$$z\equiv z_1,\quad z\equiv z_2,\quad z\equiv z_3, \text{ etc. } (\text{mod } p^{\mu+\nu}).$$

Then it is clear that if z_i is a quadratic residue of $p^{\mu+\nu}$, and if $x^2\equiv z_i \ (\text{mod } p^{\mu+\nu})$, the value of

$$\frac{m-ax^2}{b},$$

is an integer congruent to n_i (mod p^μ), and therefore cannot be a square. Conversely, if we suppose that

$$\frac{m-ax^2}{b}\equiv n_i \ (\text{mod } p^\mu),$$

we have

$$ax^2\equiv m-bn_i \ (\text{mod } p^{\mu+\nu})$$
$$\equiv az_i,$$

and therefore

$$x^2\equiv z_i.$$

If, then, ζ, ζ', ζ'', etc. are those of the numbers z_i which are quadratic residues of $p^{\mu+\nu}$, and if $\pm\xi$, $\pm\xi'$, $\pm\xi''$, etc. are the solutions of the congruences

$$x^2\equiv\zeta,\quad x^2\equiv\zeta',\quad x^2\equiv\zeta'', \text{ etc. } (\text{mod } p^{\mu+\nu}),$$

it follows that no values of x which are congruent (mod $p^{\mu+\nu}$) to any of the numbers $\pm\xi$, $\pm\xi'$, $\pm\xi''$, etc. can possibly lead to integral solutions of the proposed equation.

In most cases ν will be zero; and in applying the method we may put successively $\mu=1, 2, 3$, etc., and then for any particular value of μ it is sufficient to retain those non-residues (n_i) of p^μ which are residues of lower powers of p, since those which are non-residues of lower powers lead to values of x which have been already excluded.

The value of x must in any case be less than $\sqrt{m/a}$; and by the process of exclusion just explained the number of values which have to be tried may be reduced to any extent that may be desired.

As an application, let it be required to factorise 781727. It will be found that this number, which is of the form $4n+3$, is a non-residue of 3 and a residue of 59: this agrees with the generic character of the form (3, 0, 59), for which $\Delta = 177$, one of the sixty-five special determinants given above.

We now proceed to find all the positive integral solutions of

$$59x^2 + 3y^2 = 781727.$$

It will be observed in the first place that $x < 116$, and that $x^2 \equiv 1 \pmod 3$, or $x \equiv \pm 1 \pmod 3$. Within the prescribed limits there are 77 numbers of these forms, namely

$$1, 2, 4, 5 \ldots 113, 115.$$

Now take the 'excluding number' 5; then since $59 \equiv -1 \pmod 5$ and $781727 \equiv 2 \pmod 5$, while the non-residues of 5 are 2 and 3, we have to solve the auxiliary congruences

$$-z + 6 \equiv 2, \quad -z + 9 \equiv 2 \pmod 5,$$

whence $$z_1 \equiv 4, \qquad z_2 \equiv 2 \pmod 5.$$

The first of these leads to the exclusion of all values of x which are of the forms $5n \pm 2$.

In a similar way the excluding numbers 7, 11, 13 lead to the rejection of all values of x which are of the forms

$$7n,\ 7n \pm 2;\ 11n \pm 1,\ 11n \pm 2;\ 13n,\ 13n \pm 5,\ 13n \pm 6;$$

after which only the following twelve remain:—

$$4,\ 11,\ 25,\ 29,\ 41,\ 71,\ 74,\ 80,\ 94,\ 95,\ 106,\ 115.$$

It is easily seen that x cannot be a multiple of 4, so that 4 and 80 may be rejected; then by actual trial of the remaining values we find that

$$\begin{aligned} 781727 &= 59 \,.\, 29^2 + 3 \,.\, 494^2 \\ &= 59 \,.\, 74^2 + 3 \,.\, 391^2 \\ &= 59 \,.\, 115^2 + 3 \,.\, 22^2. \end{aligned}$$

Since these representations are all primitive, we conclude that 781727 is the product of three different primes.

To find the actual values of the factors, we observe that since

$$\left.\begin{aligned} 3\,.\,494^2 + 59\,.\,29^2 \equiv 0 \\ 3\,.\,22^2 + 59\,.\,115^2 \equiv 0 \end{aligned}\right\} \pmod{781727},$$

it follows that $\qquad 3\,(494^2\,.\,115^2 - 22^2\,.\,29^2) \equiv 0.$

Now $494\,.\,115 - 22\,.\,29 = 56172$, and it will be found that $dv\,(56172, 781727) = 4681$. Hence also $781727 \div 4681 = 167$, which is a prime. The other prime factors may be found in a similar way, and the final result is that

$$781727 = 31\,.\,151\,.\,167.$$

215. In general, suppose that

$$ax^2 + by^2 = m,$$
$$ax'^2 + by'^2 = m,$$

where, as before, a, b are positive and prime to each other and to m. For simplicity, take x, y, x', y' all positive. Then

$$\begin{aligned} a\,(xy' + x'y)\,(xy' - x'y) &= (y'^2 - y^2)\,m \\ &\equiv 0 \pmod{m} \end{aligned}$$

Therefore one of the numbers $(xy' + x'y)$, $(xy' - x'y)$ is a multiple of m, or else each of them has a factor in common with m.

Now $\qquad$ $$\begin{aligned} m^2 &= (ax^2 + by^2)\,(ax'^2 + by'^2) \\ &= (axx' - byy')^2 + ab\,(xy' + x'y)^2 : \end{aligned}$$

therefore, except when $ab = 1$, $(xy' + x'y)$ is certainly less than m, and hence $dv\,(m, xy' + x'y)$ is a factor of m.

If $ab = 1$, then $a = b = 1$, and

$$m^2 = (xx' - yy')^2 + (xy' + x'y)^2,$$

and here again $xy' + x'y < m$ except when

$$x' : y' = y : x,$$

which leads to $x' = y$, $y' = x$. If we consider that, from our present point of view, the representations $m = x^2 + y^2$ and $m = y^2 + x^2$ are not distinct, we may say that in every case two distinct positive solutions of $ax^2 + by^2 = m$ lead to the determination of a factor of m.

The more general equation

$$ax^2 + 2bxy + cy^2 = m,$$

may be replaced by $\qquad (ax + by)^2 + \Delta y^2 = am,$

and then treated by the method already explained. If (x, y), (x', y') are two different positive solutions, then it may be shown that $dv\,(xy' + x'y, m)$ is a factor of m.

It should also be observed that in finding, by this method of trial, all the solutions of $ax^2 + 2bxy + cy^2 = m$, derived as well as primitive solutions are included. Every derived representation gives a square factor of m; and moreover, if (a, b, c) is a form by which m may be primitively represented, and if δ^2 is any square factor of m, the genus to which (a, b, c) belongs will certainly contain a form by which m/δ^2 can be primitively represented, or, in other words, which will give a derived representation of m. Therefore by applying Gauss's method to all the representative forms of the genus, we are able to detect all the square divisors of m, and the factorisation of m is completely effected.

Gauss has given an auxiliary table (Werke, ii. pp. 507—9) to facilitate the solution of $ax^2 + by^2 = m$; and in the *Disquisitiones* (*l. c.*) will be found some practical rules for still further shortening the work.

Tables of definite forms, suitable for the factorising of large numbers, are given by Seelhoff (*Amer. Journ.* vii. p. 264, and viii. p. 26). In another paper (*ibid.* viii. p. 39), Seelhoff has explained a method of reducing a given number m to the form $x^2 \pm Dy^2$, which is substantially as follows.

Let a be the greatest integer in $\sqrt{m}$, and put

$$m = a^2 + b.$$

Find an odd prime p of which m is a quadratic residue: then m is also a quadratic residue of p^2, and the solution of

$$x^2 \equiv m \pmod{p^2},$$

will be of the form $$x \equiv \pm \xi \pmod{p^2}.$$

More generally, if m is a quadratic residue of the different odd primes p, q, r, etc., and if P involves no other prime factors but these, it will be possible to solve the congruence

$$x^2 \equiv m \pmod{P^2},$$

and if $$x = P^2y + \xi$$

is any solution of it, $$m - x^2 \equiv 0 \pmod{P^2},$$

and therefore $$m = x^2 \pm nP^2$$

where n is some integer. It will generally be most convenient to choose x so that $m - x^2$ may be as small as possible, in order that n may be comparatively small. In other words, y must be taken so that the numerical value of $P^2y + \xi$ is as near as possible to a.

So long as $P^2 < 2a$, it will be possible to make x less than a, and the corresponding representation

$$m = x^2 + nP^2$$

is one to which Gauss's method may be applied. In every case we obtain a quadratic residue of m, and this may be utilised as already explained.

Seelhoff's method is especially valuable when m is very large; and it should be observed that it may be applied to multiples of m as well as to m itself.

216. Tchébicheff has shewn (Liouville (1), xvi. p. 257) that if a number m can be represented by an indefinite form $\pm(x^2 - Dy^2)$, the determination of the factors of m may be effected by considering all the representations in which the variables x, y are restricted within certain limits.

Suppose that $$\xi^2 - D\eta^2 = m$$

is any representation of m by the form $(1, 0, -D)$, and that ξ, η are taken to be positive.

Then if (T, U) is the fundamental solution of $T^2 - DU^2 = 1$, we obtain another representation

$$\xi'^2 - D\eta'^2 = m,$$

by putting $$\xi' = \pm(T\xi - DU\eta)$$
$$\eta' = \pm(U\xi - T\eta).$$

Now $$T\xi - DU\eta = \sqrt{(1 + DU^2)(m + D\eta^2)} - DU\eta > 0;$$
so that to make ξ' positive we must take the upper sign in the ambiguity.

The condition that ξ' may be less than ξ gives

$$DU\eta > (T - 1)\xi,$$

and therefore $$DU^2(\xi^2 - m) > (T - 1)^2\xi^2,$$

leading to $$2(T - 1)\xi^2 > mDU^2$$
$$> m(T^2 - 1);$$

and hence $$\xi > \sqrt{\frac{(T + 1)m}{2}}.$$

Conversely, if this condition is satisfied, $\xi' = T\xi - DU\eta$ will be positive and less than ξ; so that if the equation $x^2 - Dy^2 = m$ is capable of solution there will be a suitable value of x which is positive and less than $\sqrt{\frac{(T+1)m}{2}}$. The corresponding value of y will be less than that given by

$$Dy^2 = \frac{(T+1)m}{2} - m = \frac{(T-1)m}{2};$$

that is, it will be less than $\sqrt{\frac{(T-1)m}{2D}}$.

In the same way, if the equation

$$x^2 - Dy^2 = -m$$

admits of solution, then by writing it in the form

$$(Dy)^2 - Dx^2 = mD,$$

we see as before that there will be a value of x which is positive and less than $\sqrt{\frac{(T-1)m}{2}}$, and that the corresponding positive value of y is less than $\sqrt{\frac{(T+1)m}{2D}}$.

Suppose, now, that there are two representations

$$x_1^2 - Dy_1^2 = m, \qquad x_2^2 - Dy_2^2 = m,$$

such that

$$0 < x_1 < \sqrt{\frac{(T+1)m}{2}}, \qquad 0 < y_1 < \sqrt{\frac{(T-1)m}{2D}},$$

$$0 < x_2 < \sqrt{\frac{(T+1)m}{2}}, \qquad 0 < y_2 < \sqrt{\frac{(T-1)m}{2D}};$$

then
$$(x_1x_2 + Dy_1y_2)^2 - D(x_1y_2 + x_2y_1)^2 = m^2,$$
and if we suppose that $(x_1y_2 + x_2y_1)$ is a multiple of m we have

$$\left(\frac{x_1x_2 + Dy_1y_2}{m}\right)^2 - D\left(\frac{x_1y_2 + x_2y_1}{m}\right)^2 = 1,$$

and therefore $(x_1x_2 + Dy_1y_2)/m$ is an integer.

But
$$x_1x_2 + Dy_1y_2 < \frac{(T+1)m}{2} + \frac{(T-1)m}{2}$$
$$< mT;$$

hence if we put

$$\frac{x_1x_2 + Dy_1y_2}{m} = t, \qquad \frac{x_1y_2 + x_2y_1}{m} = u,$$

we have $t^2 - Du^2 = 1$, with $t < T$, and u not zero; but this is impossible, therefore $x_1y_2 + x_2y_1$ cannot be a multiple of m.

In the same way it may be inferred from

$$(x_1x_2 - Dy_1y_2)^2 - D(x_1y_2 - x_2y_1)^2 = m^2,$$

that $(x_1y_2 - x_2y_1)$ cannot be a multiple of m.

But

$$\begin{aligned}(x_1y_2 + x_2y_1)(x_1y_2 - x_2y_1) &= x_1^2y_2^2 - x_2^2y_1^2\\ &= (m + Dy_1^2)\,y_2^2 - (m + Dy_2^2)\,y_1^2\\ &= (y_2^2 - y_1^2)\,m\\ &\equiv 0 \pmod{m},\end{aligned}$$

therefore m must be composite, and $dv\,(x_1y_2 \pm x_2y_1,\, m)$ gives a factor of m.

The same reasoning applies when there are two different solutions of $x^2 - Dy^2 = -m$. The investigation may be summed up as follows:—

If the equation $x^2 - Dy^2 = \pm m$ admits of two distinct positive solutions $(x_1, y_1)\,(x_2, y_2)$ such that

$$x_i < \sqrt{\frac{(T \pm 1)\,m}{2}}, \qquad y_i < \sqrt{\frac{(T \mp 1)\,m}{2D}},$$

the number m is certainly composite, and $dv\,(x_1y_2 \pm x_2y_1, m)$ will be a factor of m.

In the memoir above quoted, Tchébicheff has given a list of quadratic forms $\pm(x^2 - Dy^2)$ with the linear forms of m which are appropriate to each. When a suitable form has been found, the representations of m within the prescribed limits may be discovered by a tentative method, such as that of exclusion.

In spite of all that has been done hitherto, the determination of the factors of a very large number is extremely laborious. It is possible that the development of the theory of arithmetical forms of higher degrees may throw some additional light upon the subject.

On the general indeterminate equation of the second degree, the reader may consult:

Euler: *Resolutio æquationis $Ax^2 + 2Bxy + Cy^2 + 2Dx + 2Ey + F = 0$ per numeros tam rationales quam integros* (Nov. Comm. Petrop. xviii. (1773), p. 185, or Comm. Arith. i. p. 549), with the supplementary paper *De resolutione irrationalium per fractiones continuas*, etc. (ibid. p. 218, or Comm. Arith. i. p. 570).

LAGRANGE: *Sur la Solution des Problèmes Indéterminés du second degré* (Hist. de l'Acad. de Berlin for 1767, vol. xxiii. p. 165), and *Nouvelle Méthode pour résoudre les Problèmes Indéterminés en nombres entiers* (ibid. vol. xxiv. p. 181).

On the earlier researches on the discovery of prime factors, see Fermat's correspondence with Mersenne and others: also the following papers by Euler:—

Quomodo numeri præmagni sint explorandi, utrum sint primi, necne (Nov. Comm. Petr. xiii. (1768), p. 67, or Comm. Arith. i. p. 379).

De formulis speciei $mxx+nyy$ ad numeros primos explorandos idoneis, earumque mirabilibus proprietatibus (Nov. Acta Petrop. xii. p. 22, or Comm. Arith. ii. p. 249).

Extrait d'une lettre à M. Béguelin (Nouv. Mém. de l'Acad. de Berlin, 1776, p. 337, or Comm. Arith. ii. p. 270).

Many other of Euler's memoirs relate more or less to the same subject: see the analytical index prefixed to the Commentaries.

CHAPTER X.

The Distribution of Primes.

217. THE reader will have observed that, in connexion with the theories of congruences and arithmetical forms, prime numbers, speaking generally, present themselves rather as *data* than as *quæsita*; so that, from this point of view, the arithmetician regards a table of primes principally as a record of experimental facts, which he can use for the purpose of numerical applications, or in order to discover by induction, if possible, new arithmetical theorems. But the law of the succession of prime numbers has itself been the object of repeated investigation, and has led to researches of great interest and novelty; it seems right, therefore, to give some account of what has been done in this direction, although, from the nature of the case, the present chapter must appear out of harmony with its surroundings.

The tabulation of primes is effected by a merely mechanical process, which is equivalent to that of writing down the series of natural numbers in order, and successively erasing the multiples of 2, of 3, of 5, etc. after which the numbers which remain are obviously primes. For an account of the actual method by which this 'sifting' is carried out, the reader may consult a paper by J. W. L. Glaisher in the Report of the British Association for 1878 (p. 173); the introductions, by J. Glaisher, to the factor-tables for the 4th, 5th, and 6th millions, contain additional information bearing upon the subject, and a valuable bibliography.

A question of greater theoretical interest is that of determining, without previous tabulation, the number of primes which do not exceed a given limit; and this, again breaks up into two problems which are practically distinct. The first is that of actually calculating the number of primes which do not exceed a certain assigned integer, say 10,000 or 1,000,000; the other is that of discovering an analytical formula which shall exactly or asymptotically represent the number of primes which do not exceed an indefinite integer n. The distinction is much the same as that between the numerical and the algebraical solution of equations; as might be expected, the problem first stated is the easier, and will therefore be discussed in the first place.

218. The method which has been adopted by Meissel, and in some respects generalized by Rogel, depends upon a simple observation, which is apparently due to Legendre; namely, that if $p_1, p_2, \ldots p_r$ denote different primes, and if m is any integer, then the number of integers contained in the series 1, 2, 3...m which are not divisible by any of the primes is

$$\begin{aligned} m - \left[\frac{m}{p_1}\right] - \left[\frac{m}{p_2}\right] - \left[\frac{m}{p_3}\right] - \ldots \\ + \left[\frac{m}{p_1p_2}\right] + \left[\frac{m}{p_1p_3}\right] + \left[\frac{m}{p_2p_3}\right] + \ldots \\ - \left[\frac{m}{p_1p_2p_3}\right] - \left[\frac{m}{p_1p_2p_4}\right] - \left[\frac{m}{p_2p_3p_4}\right] - \ldots \\ + \left[\frac{m}{p_1p_2p_3p_4}\right] + \ldots \end{aligned}$$

where $\left[\frac{m}{p_1}\right]$ means the integral part of $\frac{m}{p_1}$, and similarly for the rest. For convenience, this may be written

$$[m]\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\ldots\left(1-\frac{1}{p_r}\right),$$

on the understanding that the product is to be expanded and then the integral part of each term taken.

To prove this, it is sufficient to observe that if n is any integer, $\left[\frac{m}{n}\right]$ is the number of integers less than m which are multiples of n; and that if an integer k, which is less than m, is divisible by exactly λ different primes out of the set $p_1, p_2 \ldots p_r$, it has to be reckoned as a multiple of each of these primes, and of each of their products 2, 3...λ at a time: so that corresponding to it we have in the expression

$$\Sigma\left[\frac{m}{p_i}\right]-\Sigma\left[\frac{m}{p_ip_j}\right]+\ldots\ldots$$

a contribution

$$\lambda-\tfrac{1}{2}\lambda(\lambda-1)+\frac{1}{3!}\lambda(\lambda-1)(\lambda-2)-\ldots=1.$$

It follows from this that the sum above written is equal to the number of integers less than m which are divisible by one at least of the selected primes; subtracting this from m, the remainder expresses the number of integers in the series 1, 2,...m which are not divisible by any of the primes. (Compare Art. 7).

For example, the number of integers not greater than 50 which are prime to 2, 3, 5, 7 is

$$50-25-16-10-7+8+5+3+3+2+1$$
$$-1-1-0-0+0=12;$$

they are, in fact,

1, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47.

It will be sometimes convenient to write

$$\phi(m;\ p_1, p_2, \ldots p_r),$$

for the number of integers, including unity, which do not exceed m, and are not divisible by any of the primes p_1, p_2,...p_r. With this notation, we have

$$\phi(m;\ p_1, p_2\ldots p_r)=[m]\prod_1^r\left(1-\frac{1}{p_i}\right)\ \ldots\ldots\ldots\ldots(1).$$

It should be observed that when $p_1, p_2\ldots p_r$ are the different prime factors of m, this expression coincides with $\phi(m)$ as defined in Art. 7; and also that the value of the expression is not altered by adding to the series of selected primes any number of primes which exceed m, because these additional primes only contribute zero terms to the sum which has to be calculated.

It will now be supposed that p_1, p_2, p_3, etc. denote the successive primes in their natural order, so that

$$p_1=2,\quad p_2=3,\quad p_3=5,$$

and so on. Instead of $\phi(m;\ p_1, p_2, \ldots p_r)$ we shall write $\Phi(m, r)$, and we shall use $F(x)$ to denote the number of primes which do not exceed x. (Observe that x need not be an integer.)

It follows at once from the definitions that

$$\Phi(m,\ F(m)) = 1 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(2),$$

because every number, not greater than m, except unity, is divisible by one at least of the primes $p_1, p_2, \ldots p_{F(m)}$.

More generally, if n is any positive integer,

$$\Phi(m,\ F(m)+n) = 1 \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(3).$$

Let p_{a+1} be the first prime which exceeds $\sqrt{m}$, or which is the same thing, let $a = F(\sqrt{m})$; then since the only numbers in the series 1, 2,...m which are not divisible by any of the primes $p_1, p_2 \ldots p_a$ are unity and those primes which exceed $\sqrt{m}$ but not m, and the number of these primes is $F(m) - F(\sqrt{m})$, that is, $F(m) - a$, we have

$$F(m) - a + 1 = \Phi(m,\ a) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(4).$$

It is easily seen that this relation continues to hold good, provided that a is an integer satisfying the conditions

$$F(m) \nless a \nless F(\sqrt{m}) \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots(5):$$

the argument is, in fact, the same as before.

For example, if $m = 50$, $F(\sqrt{m}) = F(7) = 4$, and

$$\Phi(m,\ F(\sqrt{m})) = \Phi(50,\ 4) = 12:$$

hence $$F(50) = 12 + 3 = 15.$$

Thus, in general, the tabulation of primes up to p_a enables us to calculate the value of $F(m)$. The calculation of $\Phi(m,\ F(\sqrt{m}))$ is, however, impracticable when m is very large; it is therefore necessary to make use of a few transformations to obtain a manageable formula.

We observe, in the first place, that if x, y are positive and $y > 1$,

$$\left[\frac{x}{y}\right] = \left[\frac{[x]}{y}\right],$$

from which, and the identity

$$[m]\prod_1^n\left(1 - \frac{1}{p_i}\right) = [m]\prod_1^{n-1}\left(1 - \frac{1}{p_i}\right) - \left[\frac{m}{p_n}\right]\prod_1^{n-1}\left(1 - \frac{1}{p_i}\right),$$

it follows that

$$\Phi(m,\ n) = \Phi(m,\ n-1) - \Phi\left(\left[\frac{m}{p_n}\right],\ n-1\right) \ldots\ldots(6).$$

Put $n = a = F(\sqrt{m})$: then by (4) and (6)

$$F(m) = a - 1 + \Phi(m,\ a-1) - \Phi\left(\left[\frac{m}{p_a}\right],\ a-1\right).$$

Let $a' = F\left(\sqrt{\frac{m}{p_a}}\right)$; then, in general,

$$F\left(\frac{m}{p_a}\right) \nless a - 1 \nless a',$$

and consequently another application of (4) gives

$$\begin{aligned} F(m) &= a - 1 + \Phi(m, a-1) - F\left(\frac{m}{p_a}\right) + a - 2 \\ &= (a-1) + (a-2) - F\left(\frac{m}{p_a}\right) + \Phi(m, a-1). \end{aligned}$$

Provided that

$$F\left(\frac{m}{p_{a-1}}\right) \nless a - 2 \nless F\left(\sqrt{\frac{m}{p_{a-1}}}\right),$$

this may be again transformed in the same way into

$$\begin{aligned} F(m) = (a-1) + (a-2) + (a-3) - F\left(\frac{m}{p_a}\right) - F\left(\frac{m}{p_{a-1}}\right) \\ + \Phi(m, a-2), \end{aligned}$$

and so on, until at last we obtain

$$\left.\begin{aligned} F(m) &= (a-1) + (a-2) + \ldots + (a-\nu-1) \\ &\quad - F\left(\frac{m}{p_a}\right) - F\left(\frac{m}{p_{a-1}}\right) - \ldots - F\left(\frac{m}{p_{a-\nu+1}}\right) \\ &\quad + \Phi(m, a-\nu) \end{aligned}\right\} \ldots\ldots(7),$$

with the conditions

$$F\left(\frac{m}{p_{a-\nu+1}}\right) \nless a - \nu \nless F\left(\sqrt{\frac{m}{p_{a-\nu+1}}}\right),$$

while the inequalities

$$F\left(\frac{m}{p_{a-\nu}}\right) \nless a - \nu - 1 \nless F\left(\sqrt{\frac{m}{p_{a-\nu}}}\right),$$

are *not* satisfied.

Now since $p_{a-\nu} < p_{a-\nu+1}$ we have

$$F\left(\frac{m}{p_{a-\nu}}\right) \nless F\left(\frac{m}{p_{a-\nu+1}}\right);$$

so that if

$$F\left(\frac{m}{p_{a-\nu+1}}\right) \nless a - \nu,$$

it follows *a fortiori* that

$$F\left(\frac{m}{p_{a-\nu}}\right) \nless a - \nu - 1.$$

Consequently the only way in which the process of transformation can be stopped is when

$$a - \nu \nless F\left(\sqrt{\frac{m}{p_{a-\nu+1}}}\right),$$

while

$$a - \nu - 1 < F\left(\sqrt{\frac{m}{p_{a-\nu}}}\right).$$

Suppose now that ν is determined by the conditions

$$p^3{}_{a-\nu} \ngtr m < p^3{}_{a-\nu+1};$$

then

$$\sqrt{\frac{m}{p_{a-\nu+1}}} < p_{a-\nu+1},$$

and consequently

$$F\left(\sqrt{\frac{m}{p_{a-\nu+1}}}\right) < F(p_{a-\nu+1}) < a - \nu + 1,$$

$$\ngtr a - \nu,$$

while, since

$$\sqrt{\frac{m}{p_{a-\nu}}} \nless p_{a-\nu},$$

$$F\left(\sqrt{\frac{m}{p_{a-\nu}}}\right) \nless F(p_{a-\nu}) \nless a - \nu$$

$$> a - \nu - 1.$$

Thus the conditions of inequality cease to hold good when

$$a - \nu = F(\sqrt[3]{m}),$$

or

$$\nu = \mathrm{F}(\sqrt{m}) - F(\sqrt[3]{m});$$

and it is easily seen that they do not break down before, because whenever

$$a - \nu \nless F\left(\sqrt{\frac{m}{p_{a-\nu+1}}}\right),$$

it follows *a fortiori* that

$$a - \nu + 1 \nless F\left(\sqrt{\frac{m}{p_{a-\nu+2}}}\right).$$

If, then, we put $F(\sqrt[3]{n}) = b$, and suppose that in (7) ν has its critical value $(a - b)$, we obtain finally

$$F(m) = \tfrac{1}{2}(a - b + 1)(a + b - 2) + \Phi(m, b)$$

$$- \sum_{b+1}^{a} F\left(\frac{m}{p_i}\right) \text{ ....(8)},$$

$$[a = F(\sqrt{m}), \quad b = F(\sqrt[3]{m})].$$

As an illustration of this result, suppose $m = 50$; then

$$a = 4, \quad b = 2,$$

and the formula gives

$$\begin{aligned} F(50) &= \tfrac{1}{2} . 3 . 4 + \Phi(50, 2) \\ &\quad - \{F(10) + F(7)\} \\ &= 6 + 17 - (4 + 4) = 15, \end{aligned}$$

which is right.

In applying the formula to a large number m, $\Phi(m, b)$ is calculated by the repeated application of equation (6). For the details of the actual computation, the reader is referred to Meissel's papers; the following table gives his results:

n	$F(n)$
20000	2262
100000	9592
200000	17984
300000	25997
400000	33860
500000	41538
600000	49098
700000	56543
800000	63951
900000	71274
1000000	78498
10000000	664579
100000000	5761460

219. In a memoir presented in 1850 to the Academy of St Petersburgh, Tchébicheff determined, in an explicit analytical form, a superior and an inferior limit to the number of primes between the limits α and β, both of which are assumed to be greater than 1. Before we give an account of Tchébicheff's investigation, it may be as well to trace the connexion of ideas by which it was probably suggested.

Let $\beta > \alpha > 1$, and let μ be the number of primes which exceed α but do not exceed β; also let $\theta(x)$ denote the sum of the logarithms of all the primes which do not exceed x. Then

$$\theta(\beta) - \theta(\alpha)$$

is the sum of the logarithms of all the primes p which satisfy the conditions

$$\alpha < p \overset{=}{<} \beta,$$

and since the least of these primes exceeds α, while the greatest does not exceed β, it is clear that

$$\mu \log \alpha < \theta(\beta) - \theta(\alpha) < \mu \log \beta,$$

and therefore

$$\frac{\theta(\beta) - \theta(\alpha)}{\log \beta} < \mu < \frac{\theta(\beta) - \theta(\alpha)}{\log \alpha}.$$

The problem is therefore reduced to the determination of a superior and an inferior limit of $\theta(x)$; and this is ultimately made to depend upon Stirling's asymptotic value of Πx or $\Gamma(x+1)$.

220. Besides the function $\theta(x)$ which has been already defined, Tchébicheff considers the function $T(x)$, which denotes the sum of the logarithms of all the integers (prime and composite) which do not exceed x. If we write, for convenience, $\theta\left(\frac{x}{m}\right)^{\frac{1}{i}}$ instead of $\theta\left\{\left(\frac{x}{m}\right)^{\frac{1}{i}}\right\}$, the following relation will hold good:—

$$\begin{aligned} T(x) = \theta(x) &+ \theta(x)^{\frac{1}{2}} + \theta(x)^{\frac{1}{3}} + \theta(x)^{\frac{1}{4}} + \ldots \\ + \theta\left(\frac{x}{2}\right) &+ \theta\left(\frac{x}{2}\right)^{\frac{1}{2}} + \theta\left(\frac{x}{2}\right)^{\frac{1}{3}} + \theta\left(\frac{x}{2}\right)^{\frac{1}{4}} + \ldots \\ + \theta\left(\frac{x}{3}\right) &+ \theta\left(\frac{x}{3}\right)^{\frac{1}{2}} + \theta\left(\frac{x}{3}\right)^{\frac{1}{3}} + \theta\left(\frac{x}{3}\right)^{\frac{1}{4}} + \ldots \\ + \ldots&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \\ &= \sum_{m,\,i} \theta\left(\frac{x}{m}\right)^{\frac{1}{i}}, \end{aligned}$$

in which all the terms are to be retained which do not vanish.

To prove this, consider any prime p; its logarithm will occur once, or not at all, in the sum represented by $\theta\left(\frac{x}{m}\right)^{\frac{1}{i}}$ according as

$$\left(\frac{x}{m}\right)^{\frac{1}{i}} < p \text{ or } \left(\frac{x}{m}\right)^{\frac{1}{i}} \nless p,$$

that is, according as x is or is not less than mp^i. Hence the number of times $\log p$ will occur in the i^{th} column of the above-written double sum is $\left[\frac{x}{p^i}\right]$, and the total number of times $\log p$ will appear in the double sum is

$$\left[\frac{x}{p}\right] + \left[\frac{x}{p^2}\right] + \left[\frac{x}{p^3}\right] + \ldots$$

where, as usual, $\left[\frac{x}{p}\right]$ is the integral part of $\frac{x}{p}$, and the series is to be continued until the terms vanish.

But this is precisely the power in which p occurs in the product of all the integers which do not exceed x. In fact this product is $[x]\,!$, and the highest power of p which occurs in this is

$$\left[\frac{[x]}{p}\right] + \left[\frac{[x]}{p^2}\right] + \left[\frac{[x]}{p^3}\right] + \ldots;$$

now, since $p > 1$, $\left[\frac{[x]}{p^i}\right] = \left[\frac{x}{p^i}\right]$, and therefore the two sums last written have the same value.

Since p was any prime whatever, the proposition follows, and we have

$$T(x) = \log \Pi\,[x] = \sum_{m,\,i} \theta\left(\frac{x}{m}\right)^{\frac{1}{i}}.$$

It is convenient to write

$$\psi(x) = \theta(x) + \theta(x)^{\frac{1}{2}} + \theta(x)^{\frac{1}{3}} + \ldots$$
$$= \sum_i \theta(x)^{\frac{1}{i}};$$

and with this notation, we have

$$T(x) = \sum_m \psi\left(\frac{x}{m}\right).$$

221. We now come to the application of Stirling's theorem. By an analysis, which need not be reproduced here, Serret has proved (*Alg. Supér.* 2nd ed. p. 212, or Todhunter *Int. Calc.* Chap. 16) that

$$\log \Pi x > \tfrac{1}{2}\log 2\pi - x + (x + \tfrac{1}{2})\log x$$

and $$\log \Pi x < \tfrac{1}{2}\log 2\pi - x + (x + \tfrac{1}{2})\log x + \frac{1}{12x}.$$

In the first of these inequalities change x into $(x+1)$, and subtract $\log(x+1)$ from both sides; thus

$$\log \Pi x > \tfrac{1}{2}\log 2\pi - (x+1) + (x+\tfrac{1}{2})\log(x+1)$$
$$> \tfrac{1}{2}\log 2\pi + (x+1)\{\log(x+1) - 1\} - \tfrac{1}{2}\log(x+1).$$

Now it will be found that the expression

$$y(\log y - 1) - \tfrac{1}{2}\log y,$$

increases with y, if $y > 2$; and hence, observing that $[x] + 1 > x$, we find that, supposing $x > 1$,

$$T(x) = \log \Pi\,[x] > \tfrac{1}{2}\log 2\pi + x(\log x - 1) - \tfrac{1}{2}\log x.$$

Moreover from the second inequality, since $1 < [x] < x$, and $(y+\tfrac{1}{2})\log y - y$ increases with y, if $y > 1$, we infer that

$$T(x) < \tfrac{1}{2}\log 2\pi - x + (x+\tfrac{1}{2})\log x + \tfrac{1}{12}$$
$$< \tfrac{1}{2}\log 2\pi + x(\log x - 1) + \tfrac{1}{2}\log x + \tfrac{1}{12}.$$

Consider, now, the expression

$$\begin{aligned}
T(x) + T\left(\frac{x}{30}\right) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right)&\\
= \psi(x) + \psi\left(\frac{x}{2}\right) + \psi\left(\frac{x}{3}\right) + \psi\left(\frac{x}{4}\right) + \dots&\\
+ \psi\left(\frac{x}{30}\right) + \psi\left(\frac{x}{2\,.\,30}\right) + \psi\left(\frac{x}{3\,.\,30}\right) + \psi\left(\frac{x}{4\,.\,30}\right) + \dots&\\
- \psi\left(\frac{x}{2}\right) - \psi\left(\frac{x}{2\,.\,2}\right) - \psi\left(\frac{x}{3\,.\,2}\right) - \psi\left(\frac{x}{4\,.\,2}\right) - \dots&\\
- \psi\left(\frac{x}{3}\right) - \psi\left(\frac{x}{2\,.\,3}\right) - \psi\left(\frac{x}{3\,.\,3}\right) - \psi\left(\frac{x}{4\,.\,3}\right) - \dots&\\
- \psi\left(\frac{x}{5}\right) - \psi\left(\frac{x}{2\,.\,5}\right) - \psi\left(\frac{x}{3\,.\,5}\right) - \psi\left(\frac{x}{4\,.\,5}\right) - \dots&
\end{aligned}$$

This may evidently be reduced to the form

$$\Sigma A_n \psi\left(\frac{x}{n}\right) \qquad [n = 1, 2, 3\dots],$$

and it is easily proved that

$A_n = 1$, if n is prime to 2, 3 and 5,

$A_n = 0$, if n is divisible by one only of the factors 2, 3, 5,

$A_n = -1$ in all other cases.

For in the first case, $\psi\left(\frac{x}{n}\right)$ occurs in the top line only, and with a coefficient $+1$; in the second case, it occurs in the top line with a coefficient $+1$, and in one and only one of the other lines with a coefficient -1. If n is divisible, say, by 2 and 3, but not by 5, $\psi\left(\frac{x}{n}\right)$ will appear in the first, third and fourth rows with coefficients $+1$, -1, -1 respectively, so that on the whole the coefficient is -1, and so in the other similar cases; while if n is divisible by 2, 3 and 5, $\psi\left(\frac{x}{n}\right)$ occurs in each row with a coefficient $+1$, $+1$, -1, -1, -1 respectively, and therefore $A_n = -1$ as before.

Adopting Sylvester's convenient notation, the first thirty coefficients may be represented by the scheme

10000i100i 1i10i01i1i 001i00001i

where i is printed for -1.

Written out in full, the first part of the expression is

$$T(x) + T\left(\frac{x}{30}\right) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right)$$
$$= \psi(x) - \psi\left(\frac{x}{6}\right) + \psi\left(\frac{x}{7}\right) - \psi\left(\frac{x}{10}\right) + \psi\left(\frac{x}{11}\right) - \psi\left(\frac{x}{12}\right) + \ldots$$

It is to be observed that if $m \equiv n \pmod{30}$, $A_m = A_n$; and that the coefficients which do not vanish are alternately $+1$ and -1.

When the variable t diminishes, the function $\psi(t)$ never increases, but decreases down to zero by a series of abrupt curtailments; hence the value of the expression on the right-hand side of the identity above written cannot exceed $\psi(x)$ or fall short of $\psi(x) - \psi\left(\frac{x}{6}\right)$; therefore

$$\psi(x) - \psi\left(\frac{x}{6}\right) \not> T(x) + T\left(\frac{x}{30}\right) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right) \not> \psi(x).$$

It has already been proved that

$$T(x) > \tfrac{1}{2}\log 2\pi + x\log x - x - \tfrac{1}{2}\log x,$$
$$T(x) < \tfrac{1}{2}\log 2\pi + x\log x - x + \tfrac{1}{2}\log z + \tfrac{1}{12};$$

hence

$$T(x)+T\left(\frac{x}{30}\right) > \log 2\pi + \tfrac{31}{30}\,x\log x - \frac{x}{30}\log 30 - \tfrac{31}{30}\,x$$
$$- \log x + \tfrac{1}{2}\log 30,$$

$$T(x)+T\left(\frac{x}{30}\right) < \log 2\pi + \tfrac{31}{30}\,x\log x - \frac{x}{30}\log 30 - \tfrac{31}{30}\,x$$
$$+ \log x - \tfrac{1}{2}\log 30 + \tfrac{1}{6},$$

$$T\left(\frac{x}{2}\right)+T\left(\frac{x}{3}\right)+T\left(\frac{x}{5}\right) > \tfrac{3}{2}\log 2\pi + \tfrac{31}{30}\,x\log x$$
$$- x\left\{\tfrac{1}{2}\log 2 + \tfrac{1}{3}\log 3 + \tfrac{1}{5}\log 5\right\} - \tfrac{31}{30}\,x - \tfrac{3}{2}\log x + \tfrac{1}{2}\log 30,$$

$$T\left(\frac{x}{2}\right)+T\left(\frac{x}{3}\right)+T\left(\frac{x}{5}\right) < \tfrac{3}{2}\log 2\pi + \tfrac{31}{30}\,x\log x$$
$$- x\left\{\tfrac{1}{2}\log 2 + \tfrac{1}{3}\log 3 + \tfrac{1}{5}\log 5\right\} - \tfrac{31}{30}\,x + \tfrac{3}{2}\log x - \tfrac{1}{2}\log 30 + \tfrac{1}{4}.$$

From the first and last of these four inequalities

$$T(x)+T\left(\frac{x}{30}\right)-T\left(\frac{x}{2}\right)-T\left(\frac{x}{3}\right)-T\left(\frac{x}{5}\right)$$
$$> x\left\{\tfrac{1}{2}\log 2 + \tfrac{1}{3}\log 3 + \tfrac{1}{5}\log 5 - \tfrac{1}{30}\log 30\right\}$$
$$- \tfrac{5}{2}\log x + \tfrac{1}{2}\log\frac{450}{\pi} - \tfrac{1}{4},$$

and from the other two,

$$T(x)+T\left(\frac{x}{30}\right)-T\left(\frac{x}{2}\right)-T\left(\frac{x}{3}\right)-T\left(\frac{x}{5}\right)$$
$$< x\left\{\tfrac{1}{2}\log 2 + \tfrac{1}{3}\log 3 + \tfrac{1}{5}\log 5 - \tfrac{1}{30}\log 30\right\}$$
$$+ \tfrac{5}{2}\log x - \tfrac{1}{2}\log 1800\pi + \tfrac{1}{6}.$$

We shall write A for

$$\tfrac{1}{2}\log 2 + \tfrac{1}{3}\log 3 + \tfrac{1}{5}\log 5 - \tfrac{1}{30}\log 30 = \cdot 92129202\ldots,$$

then it is clear that it follows *a fortiori* from the above inequalities that

$$Ax + \tfrac{5}{2}\log x > T(x)+T\left(\frac{x}{30}\right)-T\left(\frac{x}{2}\right)-T\left(\frac{x}{3}\right)-T\left(\frac{x}{5}\right)$$
$$> Ax - \tfrac{5}{2}\log x - 1.$$

Strictly speaking, these results are only proved for values of x which exceed 30; but it is easily verified that the two last inequalities hold when x lies between 1 and 30; therefore they are true for all values of x which exceed 1.

222. By combining these formulae with those previously obtained (p. 282) we infer that

$$\psi(x) > Ax - \tfrac{5}{2}\log x - 1$$

$$\psi(x) - \psi\left(\frac{x}{6}\right) < Ax + \tfrac{5}{2}\log x.$$

The first of these inequalities gives an inferior limit for $\psi(x)$; to deduce from the other a superior limit, we put

$$f(x) = \tfrac{6}{5}Ax + \frac{5}{4\log 6}(\log x)^2 + \tfrac{5}{4}\log x;$$

then we have

$$\psi(x) - \psi\left(\frac{x}{6}\right) < f(x) - f\left(\frac{x}{6}\right),$$

or

$$\begin{aligned}\psi(x) - f(x) &< \psi\left(\frac{x}{6}\right) - f\left(\frac{x}{6}\right)\\ &< \psi\left(\frac{x}{6^2}\right) - f\left(\frac{x}{6^2}\right)\\ &< \ldots\ldots\ldots\ldots\ldots\\ &< \psi\left(\frac{x}{6^n}\right) - f\left(\frac{x}{6^n}\right),\end{aligned}$$

where n is any positive integer.

Now choose n so that x lies between 6^{n-1} and 6^n; then

$$\psi\left(\frac{x}{6^n}\right) = 0,$$

and it can be proved that

$$-f\left(\frac{x}{6^n}\right) < 1;$$

in fact, we have identically

$$\begin{aligned}-f(z) &= \frac{5\log 6}{16} - \frac{5}{4\log 6}(\log z + \tfrac{1}{2}\log 6)^2 - \tfrac{6}{5}Az\\ &< \frac{5\log 6}{16}, \text{ if } z \text{ is positive,}\\ &< 1 \textit{ a fortiori.}\end{aligned}$$

Hence it follows that

$$\psi(x) - f(x) < 1,$$

that is,

$$\psi(x) < \tfrac{6}{5}Ax + \frac{5}{4\log 6}(\log x)^2 + \tfrac{5}{4}\log x + 1;$$

and a superior limit of $\psi(x)$ has therefore been found.

223. It is now possible to assign limits to the value of $\theta(x)$. By definition,

$$\psi(x) = \theta(x) + \theta(x)^{\frac{1}{2}} + \theta(x)^{\frac{1}{3}} + \dots$$

and therefore

$$\psi(x) - \psi(x^{\frac{1}{2}}) = \theta(x) + \theta(x)^{\frac{1}{3}} + \theta(x)^{\frac{1}{5}} + \dots$$
$$\nless \theta(x),$$

and

$$\psi(x) - 2\psi(x^{\frac{1}{2}}) = \theta(x) - \{\theta(x)^{\frac{1}{2}} - \theta(x)^{\frac{1}{3}}\} - \{\theta(x)^{\frac{1}{4}} - \theta(x)^{\frac{1}{5}}\} - \dots$$
$$\ngtr \theta(x).$$

As already proved,

$$\psi(x) > Ax - \tfrac{5}{2}\log x - 1,$$
$$\psi(x^{\frac{1}{2}}) < \tfrac{6}{5}Ax^{\frac{1}{2}} + \frac{5}{16\log 6}(\log x)^2 + \tfrac{5}{8}\log x + 1:$$

hence

$$\psi(x) - 2\psi(x^{\frac{1}{2}}) > Ax - \tfrac{12}{5}Ax^{\frac{1}{2}} - \frac{5}{8\log 6}(\log x)^2 - \tfrac{15}{4}\log x - 3,$$

and comparing this with

$$\theta(x) \nless \psi(x) - 2\psi(x^{\frac{1}{2}}),$$

we have

$$\theta(x) > Ax - \tfrac{12}{5}Ax^{\frac{1}{2}} - \frac{5}{8\log 6}(\log x)^2 - \tfrac{15}{4}\log x - 3.$$

In a similar way it will be found that

$$\theta(x) < \tfrac{6}{5}Ax - Ax^{\frac{1}{2}} + \frac{5}{4\log 6}(\log x)^2 + \tfrac{5}{2}\log x + 2.$$

For convenience let these last inequalities be written

$$\theta(x) > \phi_1(x), \quad \theta(x) < \phi_2(x);$$

then if α, β are two positive integers such that $1 < \alpha < \beta$,

$$\theta(\beta) - \theta(\alpha) > \phi_1(\beta) - \phi_2(\alpha),$$
$$\theta(\beta) - \theta(\alpha) < \phi_2(\beta) - \phi_1(\alpha).$$

It has been remarked at the beginning of the investigation that if μ is the number of primes between α and β

$$\mu > \frac{\theta(\beta) - \theta(\alpha)}{\log\beta},$$
$$\mu < \frac{\theta(\beta) - \theta(\alpha)}{\log\alpha};$$

consequently

$$\mu > \frac{\phi_1(\beta) - \phi_2(\alpha)}{\log\beta},$$

$$\mu < \frac{\phi_2(\beta) - \phi_1(\alpha)}{\log\alpha}.$$

By putting $\alpha = 2$, we obtain superior and inferior limits for $F(\beta)$; but in order to secure a practical approximation, it is best to suppose that α and β are both large. The expressions for the limits of μ are very complicated; the essential point is that $\phi_1(\beta)$ and $\phi_2(\beta)$ are of the form $P\beta - Q\beta^{\frac{1}{2}} + R(\log\beta)$, where P, Q are constants, and $R(\log x)$ is a quadratic function of $\log x$ with numerical coefficients.

There will be more than k primes between α and β if

$$k\log\beta < \phi_1(\beta) - \phi_2(\alpha).$$

Now

$$\begin{aligned}\phi_1(\beta) - \phi_2(\alpha)& \\ &= A(\beta - \tfrac{6}{5}\alpha) - A(\tfrac{12}{5}\beta^{\frac{1}{2}} - \alpha^{\frac{1}{2}}) \\ &\quad - \frac{5}{8\log 6}\{(\log\beta)^2 + 2(\log\alpha)^2\} - \tfrac{5}{4}(3\log\beta + 2\log\alpha) - 5 \\ &> A(\beta - \tfrac{6}{5}\alpha) - \tfrac{12}{5}A\beta^{\frac{1}{2}} - \frac{15}{8\log 6}(\log\beta)^2 - \tfrac{25}{4}\log\beta - 5,\end{aligned}$$

since, by hypothesis, $\beta > \alpha$.

A fortiori, therefore, μ will exceed k, if

$$\begin{aligned}k\log\beta < A(\beta - \tfrac{6}{5}\alpha) - \tfrac{12}{5}A\beta^{\frac{1}{2}}& \\ &- \frac{15}{8\log 6}(\log\beta)^2 - \tfrac{25}{4}\log\beta - 5,\end{aligned}$$

or

$$\begin{aligned}\alpha < \tfrac{5}{6}\beta - 2\beta^{\frac{1}{2}} - \frac{16A\log 6}{25}(\log\beta)^2& \\ &- \frac{5}{6A}(\tfrac{25}{4} + k)\log\beta - \frac{25}{6A}.\end{aligned}$$

In particular, putting $k = 0$, there will be at least one prime between α and β if

$$\alpha < \tfrac{5}{6}\beta - 2\beta^{\frac{1}{2}} - \frac{25}{16A\log 6}(\log\beta)^2 - \frac{125}{24A}\log\beta - \frac{25}{6A}.$$

224. Tchébicheff employs this result to prove a theorem the truth of which was conjectured by Bertrand (*Journ. de l'École Polyt. cah.* 30); namely that there is always at least one prime between α and $2\alpha - 2$ if $\alpha > \frac{7}{2}$.

In the inequality at the end of last article, put $\beta = 2\alpha - 3$; then it becomes

$$\alpha < \tfrac{5}{6}(2\alpha - 3) - 2\sqrt{2\alpha - 3} - \frac{25}{16A \log 6}\{\log(2\alpha - 3)\}^2$$

$$- \frac{125}{24A}\log(2\alpha - 3) - \frac{25}{6A}.$$

Since, when x becomes indefinitely large, $(\log x)^2/x$ ultimately vanishes, it is easily seen that this inequality holds good for all values of α which exceed a certain finite value. This limiting value is found by changing the inequality into an equation and finding its greatest positive root. According to Tchébicheff, this lies between 159 and 160; Bertrand's postulate is therefore proved for all values of α which exceed 159, and it is easily verified for all smaller integral values except 1, 2 and 3 by actual experiment.

225. The crucial point of the investigation is where the inferior and superior limits of $\psi(x)$ are deduced from the expression

$$T(x) + T\left(\frac{x}{30}\right) - T\left(\frac{x}{2}\right) - T\left(\frac{x}{3}\right) - T\left(\frac{x}{5}\right);$$

for convenience this may be denoted, after Sylvester, by

$$[1,\ 30;\ 2,\ 3,\ 5],$$

and, in general,

$$[a_1,\ a_2, \ldots a_m;\ b_1,\ b_2, \ldots b_n],$$

may be written for

$$\sum_1^m T\left(\frac{x}{a_i}\right) - \sum_1^n T\left(\frac{x}{b_i}\right).$$

The advantage derived from the use of the combination

$$[1,\ 30;\ 2,\ 3,\ 5]$$

is twofold; in the first place, when the expression is written in the form

$$\Sigma A_n \psi\left(\frac{x}{n}\right),$$

the coefficients which do not vanish are alternately $+1$ and -1, and this leads to the determination of a superior *and* an inferior limit of $\psi(x)$; and in the second place, on account of the relation

$$1 + \tfrac{1}{30} = \tfrac{1}{2} + \tfrac{1}{3} + \tfrac{1}{5},$$

the term $x \log x$, which occurs in the limiting expressions for

$T(x)$, etc., is eliminated. The expressions for the limiting values of $[1, 30; 2, 3, 5]$ or $\Sigma A_n\psi\left(\frac{x}{n}\right)$ consequently assume the forms

$$Ax + R_1(\log x),$$

and

$$Ax + R_2(\log x),$$

where, as above,

$$A = \tfrac{1}{2}\log 2 + \tfrac{1}{3}\log 3 + \tfrac{1}{5}\log 5 - \tfrac{1}{30}\log 30,$$

and $R_1(\log x)$, $R_2(\log x)$ are rational linear functions of $\log x$.

It is evident that similar results may be obtained from the expression $[a_1, a_2, \dots a_m; b_1, b_2, \dots b_n]$ provided that

$$\sum_1^m \frac{1}{a_i} = \sum_1^n \frac{1}{b_i};$$

in fact, it will be found that

$$[a_1, a_2, \dots a_m; b_1, b_2, \dots b_n] > Ax - \frac{m+n}{2}\log x + B$$

$$< Ax + \frac{m+n}{2}\log x + B',$$

where

$$A = \Sigma\left(\frac{1}{a_i}\log a_i\right) - \Sigma\left(\frac{1}{b_i}\log b_i\right),$$

and B, B' are certain numerical constants, which may, if we think fit, be replaced by positive or negative integers, appropriately chosen.

The function $[a_1, a_2, \dots a_m; b_1, b_2, \dots b_n]$, or $[a; b]$ say, may be expanded in the form

$$\Sigma C_r\psi\left(\frac{x}{r}\right), \qquad [r = 1, 2, 3, \dots],$$

where the coefficient C_r will depend upon the relation of r to the a's and the b's; in fact, if r is divisible by p of the a's and by q of the b's, $C_r = p - q$. Hence if μ is the least common multiple of $a_1, a_2, \dots a_m, b_1, b_2, \dots b_n$ it follows that $C_s = C_r$ when $s \equiv r \pmod{\mu}$. Consequently the coefficients form a recurring series with μ terms (or fewer) in its period. The sum of the first r coefficients is easily seen to be

$$\left[\frac{r}{a_1}\right] + \left[\frac{r}{a_2}\right] + \dots + \left[\frac{r}{a_m}\right] - \left[\frac{r}{b_1}\right] - \left[\frac{r}{b_2}\right] - \dots - \left[\frac{r}{b_n}\right].$$

Call this S_r: then

$$S_\mu = \mu \left\{ \frac{1}{a_1} + \frac{1}{a_2} + \ldots + \frac{1}{a_m} - \frac{1}{b_1} - \frac{1}{b_2} - \ldots - \frac{1}{b_n} \right\}$$
$$= 0.$$

Therefore in the series

$$S_1,\ S_2, \ldots\ldots S_\mu,$$

there will be one term which is negative, and numerically greater than any of the negative terms which precede it, while it is not numerically less than any of the terms which follow it[1]. Let this be S_h; then it is easy to see that none of the expressions

$$C_{h+1},\ (C_{h+1} + C_{h+2}),\ (C_{h+1} + C_{h+2} + C_{h+3})$$
$$\ldots\ldots(C_{h+1} + C_{h+2} + \ldots + C_{h+\mu}),$$

can be negative. Remembering that $\psi(z)$ is never negative, and cannot increase when z diminishes, we infer that

$$\sum_{h+1}^{h+\mu} C_r \psi\left(\frac{x}{r}\right),$$

cannot be negative. In the same way the sum of the next group of μ terms, namely

$$\sum_{h+\mu+1}^{h+2\mu} C_r \psi\left(\frac{x}{r}\right),$$

is not negative, and so on. Therefore

$$[a;\ b] = \sum_1^h C_r \psi\left(\frac{x}{r}\right) + P,$$

where P is certainly not negative.

Comparing this with the inequality

$$[a;\ b] < Ax + \frac{m+n}{2} \log x + B',$$

we conclude that

$$\sum_1^h C_r \psi\left(\frac{x}{r}\right) < Ax + \frac{m+n}{2} \log x + B' \ \ldots\ldots\ldots\ldots\ldots \text{(i)}.$$

In the same way, if S_k is the first of the sums S_1, S_2, S_3... to attain the maximum positive value, we find that

$$[a;\ b] = \sum_1^k C_r \psi\left(\frac{x}{r}\right) - Q,$$

where Q is not negative; and hence that

$$\sum_1^k C_r \psi\left(\frac{x}{r}\right) > Ax - \frac{m+n}{2} \log x + B \ \ldots\ldots\ldots\ldots \text{(ii)}.$$

[1] It may exceptionally happen that $S_k = 0$: this is the case, for instance, with [1, 30; 2, 3, 5].

226. We will now suppose, for simplicity, that $a_1 = 1$. Each of the inequalities (i) and (ii) involves $\psi(x)$, and a certain finite number of terms $C_r\psi\left(\frac{x}{r}\right)$ besides. For these other terms may be substituted their inferior or superior limits as found by previous approximations; the inferior or superior limit being put in for each term in such a way as to leave each inequality valid. For instance, if in (i) a particular term $C_r\psi\left(\frac{x}{r}\right)$ is positive we must substitute for $\psi\left(\frac{x}{r}\right)$ its inferior limit, while if C_r is negative the superior limit of $\psi\left(\frac{x}{r}\right)$ must be inserted. Exactly the opposite rule must be applied in (ii).

When this has been done, the resulting inequalities give two new superior and inferior limits for $\psi(x)$, and these may afford closer asymptotic values for $\frac{\psi(x)}{x}$ than any previously obtained.

When h and k are inconveniently large, simplicity is gained by first suppressing on the left-hand side of (i) any group of terms (not including $\psi(x)$) which is known by previous approximations to be ultimately positive when x is very large; and in the same way in (ii) we may suppress any group of terms the value of which is known to be ultimately negative.

If, as we suppose, the first asymptotic limits adopted are those of Tchébicheff, derived from [1, 30; 2, 3, 5], it is evident that the result of any finite[1] number of applications of the process just explained will be of the form

$$\begin{aligned}\psi(x) &> Ax + Q_1(\log x)\\ &< A'x + Q_2(\log x),\end{aligned}$$

where A, A' are constants, and $Q_1(\log x)$, $Q_2(\log x)$ are rational integral functions of $\log x$ not exceeding the second degree.

Since $\log x$ and $(\log x)^2$ are both negligible in comparison with x, when x is very large, we may consider that A and A' are asymptotic limits of $\frac{\psi(x)}{x}$, and the nearness of the approximation may be estimated by the approach of A'/A to unity. This ratio A'/A is called by Sylvester, to whom this extension of Tchébi-

[1] We say *finite*, in order to avoid the risk of the coefficients of $Q_1(\log x)$ or $Q_2(\log x)$ becoming infinite.

cheff's theory is due, the *regulator* of the approximation. Thus Tchébicheff's original process gives a regulator $\frac{6}{5} = 1{\cdot}2$.

227. The choice of groups of selected terms which may be omitted from Sylvester's inequalities is much facilitated by the following considerations. Suppose that at any stage of the approximation we have obtained asymptotic values for $\psi(x)$ in the form

$$\begin{aligned}\psi(x) &> Ax + Q_1(\log x)\\ &< qAx + Q_2(\log x),\end{aligned}$$

so that q is the regulator.

Let m, μ be positive integers, and $m < \mu$. Then we have

$$\psi\left(\frac{x}{m}\right) - \psi\left(\frac{x}{\mu}\right) > \left(\frac{1}{m} - \frac{q}{\mu}\right) Ax + Q(\log x),$$

where $Q(\log x)$ is a new quadratic function of $\log x$.

Now if $\left(\frac{1}{m} - \frac{q}{\mu}\right)$ is positive, or which is the same thing, if $\mu > qm$, we thus obtain an inferior limit for $\psi(x/m) - \psi(x/\mu)$ which is ultimately positive when x is large enough; while if $\mu < qm$, the expression on the right-hand side of the above inequality is ultimately negative when x is very large. But the expression $\psi(x/m) - \psi(x/\mu)$ can never be really negative; and the explanation of the above result is that the regulator q differs too much from unity to give any inferior limit to $\psi(x/m) - \psi(x/\mu)$ except zero. Consequently, in the left-hand side of the inequality (i) we may (and should) omit any combination of terms $\psi(x/m) - \psi(x/\mu)$ with $m < \mu$ and $\mu < qm$; and in the same way in the left-hand side of (ii) we may omit any combination $-\psi(x/m) + \psi(x/\mu)$ subject to the same conditions. This principle may obviously be extended: for instance in (i) we may omit any combination

$$\psi\left(\frac{x}{m}\right) + \psi\left(\frac{x}{m'}\right) - 2\psi\left(\frac{x}{\mu}\right),$$

if m, m' are both less than μ, while

$$\frac{1}{m} + \frac{1}{m'} < \frac{2q}{\mu},$$

and so on. It may be shewn, however, that, in order to use a given regulator q to the best advantage for the next approximation, *only* those groups of terms should be omitted which can be arranged in pairs such as $\psi(x/m) - \psi(x/\mu)$ with $m < \mu < qm$.

228. Sylvester has also explained a method of successive approximation which may be applied to one and the same inequality, before attempting to find other more favourable sets $(a_i;\ b_i)$. The principle of this will be best illustrated by applying it to Tchébicheff's original result

$$[1,\ 30;\ 2,\ 3,\ 5] = \psi(x) - \psi\left(\frac{x}{6}\right) + \psi\left(\frac{x}{7}\right) - \psi\left(\frac{x}{10}\right) + \dots$$

or, as we may write it for convenience,

$$\begin{aligned} V = (1) - (6) + (7) - (10) + (11) - (12) + (13) - (15) \\ + (17) - (18) + (19) - (20) + (23) - (24) \\ + (29) - (30) + (31) - \dots \end{aligned}$$

Taking Tchébicheff's asymptotic limits, with the regulator 1·2, and omitting the groups

$$-(6) + (7),\ -(10) + (11),\ -(12) + (13), \dots -(20) + (23),$$

which are certainly not positive, although the regulator 1·2 gives us no asymptotic value for them below zero, we infer that

$$V = (1) - (24) + (29) - \epsilon,$$

where ϵ is certainly not negative.

Now $$V > Ax - \tfrac{5}{2} \log x - 1\ ;$$

therefore

$$\psi(x) > Ax - \tfrac{5}{2} \log x - 1 + \psi\left(\frac{x}{24}\right) - \psi\left(\frac{x}{29}\right).$$

Also $$\psi\left(\frac{x}{24}\right) > \frac{Ax}{24} - \tfrac{5}{2}(\log x - \log 24) - 1,$$

$$\begin{aligned} \psi\left(\frac{x}{29}\right) < \frac{6Ax}{5\,.\,29} + \frac{5}{4 \log 6}(\log x - \log 29)^2 \\ + \tfrac{5}{4}(\log x - \log 29) + 1, \end{aligned}$$

therefore *a fortiori*

$$\psi(x) > p_1 Ax + q_1 (\log x)^2 + r_1 \log x + s_1,$$

where p_1, q_1, r_1, s_1 are certain numerical constants, and in particular

$$p_1 = 1 + \tfrac{1}{24} - \tfrac{6}{45} = \tfrac{3481}{3480}.$$

In a similar way, since

$$V \nless (1) - (6) + (7) - (10),$$

we have

$$\psi(x) < Ax + \tfrac{5}{2} \log x + \psi\left(\frac{x}{6}\right) - \psi\left(\frac{x}{7}\right) + \psi\left(\frac{x}{10}\right),$$

and hence

$$\psi(x) < t_1 Ax + u_1 (\log x)^2 + v_1 \log x + w_1,$$

where t_1, u_1, v_1, w_1 are numerical constants, and in particular

$$t_1 = 1 + \tfrac{6}{5}\left(\tfrac{1}{6} + \tfrac{1}{10}\right) - \tfrac{1}{7} = \tfrac{206}{175}.$$

We may now repeat the process, employing the new asymptotic values of $\psi\left(\frac{x}{24}\right)$, $\psi\left(\frac{x}{29}\right)$, etc.; and it is clear that after i successive applications, we shall obtain results of the form

$$\psi(x) > p_i Ax + q_i (\log x)^2 + r_i \log x + s_i,$$
$$\psi(x) < t_i Ax + u_i (\log x)^2 + v_i \log x + w_i.$$

To determine the coefficients we have a set of linear difference equations with constant coefficients; these have been completely worked out by Hammond. It will be sufficient here to consider those which are satisfied by the coefficients p_i, t_i. It is easily seen that

$$\begin{aligned} p_{i+1} &= \tfrac{1}{24} p_i - \tfrac{1}{29} t_i + 1, \\ t_{i+1} &= \left(\tfrac{1}{6} + \tfrac{1}{10}\right) t_i - \tfrac{1}{7} p_i + 1 \\ &= \tfrac{4}{15} t_i - \tfrac{1}{7} p_i + 1. \end{aligned}$$

The initial values, obtained from Tchébicheff's inequalities, are

$$p_0 = 1, \qquad t_0 = \tfrac{6}{5};$$

and the complete solution is

$$p_i = \tfrac{51072}{50999} + P\rho^i + Q\rho_1{}^i,$$
$$t_i = \tfrac{59595}{50999} + R\rho^i + S\rho_1{}^i,$$

where P, Q, R, S are numerical constants, and ρ, ρ_1 are the roots of the equation

$$\left| \begin{matrix} \rho - \frac{1}{24}, & \frac{1}{29} \\ \frac{1}{7}, & \rho - \frac{4}{15} \end{matrix} \right| = 0.$$

It may be verified that ρ and ρ_1 are both proper fractions, so that the asymptotic limits of $\dfrac{\psi(x)}{x}$ obtained in this way are ultimately

$$p_\infty A = \tfrac{51072}{50999} A = 1{\cdot}0765779\ldots$$
$$t_\infty A = \tfrac{59595}{50999} A = {\cdot}9226107\ldots$$

By applying this process to the schemes

[1, 6, 70; 2, 3, 5, 7, 210]

and [1, 6, 10, 210, 231, 1155; 2, 3, 5, 7, 11, 105],

Sylvester has succeeded in reducing the inferior and superior asymptotic limits of $\frac{\psi(x)}{x}$ to

$$\cdot 9461974\ldots \text{ and } 1\cdot 0551851\ldots$$

each of which is more nearly equal to unity than the corresponding value obtained by Tchébicheff. The scheme

$$[1, 6, 10, 14, 105;\ 2, 3, 5, 7, 11, 13, 385, 1001]$$

leads to still closer limits, namely

$$\cdot 95695\ldots \text{ and } 1\cdot 04423\ldots$$

It appears to be very probable that the true asymptotic value of $\frac{\psi(x)}{x}$ is unity; of course, we cannot expect to prove that it is so by any approximative process such as that which has been described.

229. It must be carefully borne in mind that it has *not* been proved that $\frac{\psi(x)}{x}$ approximates to a definite limit when x becomes infinite; it has indeed been proved that for all values of x

$$A + \eta > \frac{\psi(x)}{x} > A' + \eta',$$

where $A = 1\cdot 04423\ldots$, $A' = \cdot 95695\ldots$ and η, η' are quantities which are very small when x is large; but this is quite consistent with the hypothesis that $\frac{\psi(x)}{x}$ continually oscillates between two finite limits, without tending to a single definite value when $x = \infty$.

It may, however, be shewn that *if* $\frac{\psi(x)}{x}$ does converge to a definite limit, this limit can only be unity. This is effected by proving that if a is any assigned quantity which is greater than 1, there is an indefinitely large number of positive integers x for which

$$\psi(x) < ax,$$

and also that if a' is any assigned quantity less than 1, there is an indefinitely large number of positive integers x for which

$$\psi(x) > a'x.$$

Poincaré's proof of this proposition is extremely simple and elegant. To avoid confusion in the use of brackets, we shall write

$E(x)$ instead of $[x]$ to denote the greatest integer which does not exceed x.

Then if the function $\alpha(x)$ is defined to mean 1 or 0 according as $x \nless 1$ or $x < 1$, we shall have

$$E(x) = \alpha(x) + \alpha\left(\frac{x}{2}\right) + \alpha\left(\frac{x}{3}\right) + \dots + \alpha\left(\frac{x}{n}\right) + \dots$$

$$= \sum_1^{x} \alpha\left(\frac{x}{n}\right);$$

in fact, since $\alpha\left(\frac{x}{n}\right) = 1$ for $n = 1, 2, 3 \dots E(x)$, while $\alpha\left(\frac{x}{n}\right) = 0$ for all integral values of n which exceed $E(x)$, the series is simply

$$1 + 1 + 1 + \dots$$

to $E(x)$ terms: that is, it is $E(x)$.

Now let $$S_n = 1 + \tfrac{1}{2} + \tfrac{1}{3} + \dots + \frac{1}{n},$$

$$V(x, n) = E(x) + E\left(\frac{x}{2}\right) + E\left(\frac{x}{3}\right) + \dots + E\left(\frac{x}{n}\right);$$

then since, if $p > 1$,

$$\frac{E(x)}{p} - 1 < E\left(\frac{x}{p}\right) < \frac{E(x)}{p},$$

it follows that

$$S_n . E(x) - n + 1 < V(x, n) < S_n . E(x) \dots\dots\dots (1).$$

Again $$\log \frac{p+1}{p} < \frac{1}{p} < \log \frac{p}{p-1},$$

and therefore $$\log(n+1) - \log 2 < S_n - 1 < \log n,$$

whence *a fortiori*

$$\log(n+1) < S_n < 1 + \log n.$$

From this and the inequalities (1) we conclude that

$$E(x) \log(n+1) - n + 1 < V(x, n) < E(x)\{1 + \log n\} \dots (2).$$

Let $$V(x) = E(x) + E\left(\frac{x}{2}\right) + \dots + E\left(\frac{x}{n}\right) + \dots$$

$$= \sum_1^{\infty} E\left(\frac{x}{n}\right);$$

then since $E\left(\frac{x}{n}\right) = 0$ if $n > E(x)$, it is clear that

$$V(x) = V\{x, E(x)\};$$

consequently by (2)

$$E(x) \log\{E(x) + 1\} - E(x) + 1 < V(x) < E(x)\{1 + \log E(x)\}.$$

Dividing by $x \log x$, and making x infinite, we see that

$$\underset{x=\infty}{\text{Lt.}} \frac{V(x)}{x \log x} = 1.$$

Now let a be any assigned quantity which is greater than 1, and suppose, if possible, that there is only a finite number of positive integers x, for which

$$\psi(x) < ax.$$

Let x_0 be the greatest of these; then for all integral values of x which exceed x_0, we shall have

$$\psi(x) \nless ax.$$

It will be possible to choose a finite positive integer b such that for *all* positive integral values of x

$$\psi(x) > a(x+1) - b;$$

we might, for instance, take $b = E\{a(x_0+1)\} + 1$.

We may infer from this, that, for all positive values of x which exceed unity,

$$\psi(x) > aE(x) - b\alpha(x):$$

in fact, if $x > 1$, we have $E(x) < x + 1$, and $\alpha(x) = 1$; on the other hand if $x < 1$ we have

$$\psi(x) = E(x) = \alpha(x) = 0.$$

In the inequality

$$\psi(x) > aE(x) - b\alpha(x)$$

change x successively into $\frac{x}{2}, \frac{x}{3}, \frac{x}{4}, \ldots$ and add; then since the inequality only fails when $\psi(x)$, $E(x)$, $\alpha(x)$ all vanish, we have

$$\sum_1^\infty \psi\left(\frac{x}{n}\right) > a\sum_1^\infty E\left(\frac{x}{n}\right) - b\sum_1^\infty \alpha(x),$$

that is,

$$T(x) > aV(x) - bE(x),$$

and therefore

$$\frac{T(x)}{x \log x} > a\,\frac{V(x)}{x \log x} - b\,\frac{E(x)}{x \log x}.$$

But from Tchébicheff's inequalities it appears that

$$\underset{x=\infty}{\text{Lt.}} \frac{T(x)}{x \log x} = 1;$$

also the limit of $E(x)/x \log x$ is zero, and that of $V(x)/x \log x$ is 1; we are therefore led to the absurd result that $1 > a$. Consequently it is impossible to assign a finite value of x_0 such that whenever $x > x_0$, $\psi(x) \nless ax_0$; the inequality

$$\psi(x) < ax$$

is therefore satisfied by an infinite number of positive integers.

It may be proved in exactly the same way that if a' is any assigned quantity less than 1, the inequality

$$\psi(x) > a'x$$

is satisfied by an infinite number of positive integers. Consequently if $\psi(x)/x$ has a definite limiting value, it must be unity.

Perhaps the argument becomes clearer with the help of a geometrical figure. Suppose the curve $y = \dfrac{\psi(x)}{x}$ to be constructed; then if A, A' are Sylvester's limits, and k, k' assigned proper fractions, however small, it has been proved that as we proceed to infinity along the axis of x, the curve ultimately lies wholly between the lines $y = A + k$, $y = A' - k'$; and also that however far we may proceed along the strip enclosed between the lines $y = 1 + m$, $y = 1 - m'$, where again m, m' are assigned positive quantities, we shall always find points of the strip which belong to the curve, no matter how small m and m' may be. Therefore if the asymptotic form of the curve is a straight line parallel to the axis of x, this line must be $y = 1$.

230. It is now easy to prove that if $\dfrac{\theta(x)}{x}$ has a definite limit when x is infinite, that limit must be unity. For suppose a is any assigned quantity greater than 1; then, by last article, the inequality $\psi(x) < ax$ is satisfied by an infinity of integral values of x; but $\theta(x) < \psi(x)$ always (Art. 220); therefore the inequality $\theta(x) < ax$ will also be satisfied by an infinity of integral values of x.

Again, for sufficiently large values of x,

$$\theta(x) > \psi(x) - 2\psi(\sqrt{x}),$$

and
$$\psi(\sqrt{x}) < \tfrac{6}{5}\sqrt{x};$$

consequently
$$\theta(x) > \psi(x) - \tfrac{12}{5}\sqrt{x},$$

or
$$\frac{\theta(x)}{x} > \frac{\psi(x)}{x} - \frac{12}{5\sqrt{x}}.$$

Now if a is any assigned quantity less than 1, there will be an infinity of integral values of x for which $\dfrac{\psi(x)}{x} > a$, and among these there will be an indefinite number for which $\frac{1}{\sqrt{x}}$ is less than assigned quantity η, however small; therefore there will be an indefinitely great number of positive integral values of x for which

$$\frac{\theta(x)}{x} > a - \eta.$$

Now if $a' < 1$, we may always put $a' = a - \eta$, where a is also less than 1 and η is positive; consequently if a' is any assigned quantity less than 1, the inequality

$$\theta(x) > a'x$$

will be satisfied by an infinite number of positive integers.

It follows, therefore, that if $\frac{\theta(x)}{x}$ converges to a definite limit, this must be unity.

231. Let $F(x)$ denote the number of primes that do not exceed x; then from the definition of $\theta(x)$ it is obvious that

$$F(x)\log x > \theta(x),$$

consequently whenever $\theta(x) > ax$, we shall have

$$F(x) > \frac{ax}{\log x}.$$

Combining this with the result of last article, we infer that whenever $a < 1$, there is an infinity of integers for which

$$F(x) > \frac{ax}{\log x}.$$

We may also prove that if $a > 1$, there is an infinity of integers for which

$$F(x) < \frac{ax}{\log x}.$$

To shew this, write, for the moment, $F(x) = n$; then because the nth prime number in order, say p_n, is greater than n, we have

$$\theta(x) = \sum_1^n \log p_r > \sum_1^n \log r$$

$$> T(n);$$

that is

$$T[F(x)] < \theta(x).$$

Now for all values of x which exceed a certain limit

$$T(x) > bx \log x,$$

where b is any assigned quantity less than 1; consequently for all such values of x

$$\theta(x) > bF(x) \log F(x).$$

But, as already proved, $F(x) \log x > \theta(x)$, and therefore

$$\log F(x) > \log \theta(x) - \log \log x;$$

hence
$$\theta(x) > bF(x) \{\log \theta(x) - \log \log x\},$$

or
$$F(x) < \frac{1}{b} \cdot \frac{\theta(x)}{\log \theta(x) - \log \log x}.$$

Let $\dfrac{y}{\log y - \log \log x} = f(y)$; then $f'(y)$ has the same sign as

$$\log y - \log \log x - 1,$$

and is therefore positive if

$$\log y > 1 + \log \log x,$$

that is, if
$$y > e \log x.$$

Provided, then, that this inequality is satisfied, $f(y)$ increases with y (x remaining constant).

Now since when x is large, $\log x$ is negligible in comparison with x, it is easily seen that both $\theta(x)$ and ax (where a is positive) exceed $e \log x$ for all values of x beyond a certain limit. Hence whenever x is sufficiently large and $\theta(x) < ax$ we shall have

$$f[\theta(x)] < f(ax),$$

that is,
$$\frac{\theta(x)}{\log \theta(x) - \log \log x} < \frac{ax}{\log(ax) - \log \log x},$$

and therefore
$$F(x) < \frac{1}{b} \cdot \frac{ax}{\log(ax) - \log \log x}.$$

When x increases indefinitely, we may write

$$\frac{ax}{\log(ax) - \log \log x} = \frac{ax}{\log x}(1 + \epsilon),$$

where ϵ ultimately vanishes. Hence if $\theta(x) < ax$, and $a' > a$, it will always be true that

$$F(x) < \frac{a'}{b} \frac{x}{\log x},$$

provided that x exceeds a certain definite value.

Now if c is any assigned quantity greater than 1, it will always be possible to assign values to a, a', b so that

$$c = \frac{a'}{b}, \quad a' > a > 1 > b,$$

and since the inequality $\theta(x) < ax$ is satisfied by an infinity of integers whenever $a > 1$, it follows that

$$F(x) < \frac{cx}{\log x}$$

for an infinity of integers, whenever c has an assigned value which exceeds unity.

We conclude, therefore, that if $\dfrac{F(x)\log x}{x}$ converges to a definite limit when x becomes infinite, that limit must be 1.

232. Legendre, in his *Théorie des Nombres*, proposed the empirical formula

$$F(x) = \frac{x}{\log x - A},$$

where

$$A = 1{\cdot}08366.$$

This agrees very fairly so long as x does not exceed a million; but as x increases, the approximation becomes more and more imperfect. Tchébicheff has proved that the least inaccurate formula of Legendre's type is

$$F(x) = \frac{x}{\log x - 1},$$

on the assumption that there is an asymptotic expression for $F(x)$ of the form

$$x\left\{\frac{a}{\log x} + \frac{b}{(\log x)^2} + \frac{c}{(\log x)^3} + \dots\right\};$$

he has also shewn that the only possible formula of this latter type, carried as far as $x/(\log x)^n$, which shall not involve an error comparable with $x/(\log x)^m$, where $m < n$, is

$$F(x) = x\left\{\frac{1}{\log x} + \frac{1}{(\log x)^2} + \frac{1\,.\,2}{(\log x)^3} + \dots + \frac{(n-1)\,!}{(\log x)^n}\right\}.$$

Thus, for instance, Legendre's corrected formula is certain to differ ultimately from $F(x)$ by quantities comparable with

$$x/(\log x)^3.$$

The infinite series

$$x\left\{\frac{1}{\log x} + \frac{1}{(\log x)^2} + \frac{2\,!}{(\log x)^3} + \dots\right\}$$

is ultimately divergent, however great x may be; but if x is very large, the sum of the first n terms will be an approximation to the integral

$$\int_\alpha^x \frac{dx}{\log x},$$

where α is any finite quantity greater than 1 and small in comparison with x. In fact, by integration by parts,

$$\int_\alpha^x \frac{dx}{\log x} = \left[\frac{x}{\log x} + \frac{x}{(\log x)^2} + \frac{2\,!\,x}{(\log x)^3} + \ldots + \frac{(n-1)\,!\,x}{(\log x)^n}\right]_\alpha^x$$
$$+ n\,!\int_\alpha^x \frac{dx}{(\log x)^{n+1}},$$

and the last term on the right is equal to

$$\frac{n\,!\,(x-\alpha)}{[\log\{\alpha+\theta(x-\alpha)\}]^{n+1}},$$

where θ is a proper fraction. When x is very large, values of n can be found for which this is a very small fraction of x. If, then, we stop at a suitable place in the infinite series, we shall obtain a value which differs from

$$\int_\alpha^x \frac{dx}{\log x}$$

only by a very small fraction of itself; x, of course, being supposed very large, and α comparatively small.

It is usual to define the logarithmic integral $li(x)$ by the equation

$$li(x) = \int_0^x \frac{dx}{\log x},$$

and say that when $x > 1$ the principal value of the integral (in Cauchy's sense) is to be taken. It is not very clear how this principal value is defined; however, there will be no objection to writing

$$\int_\alpha^x \frac{dx}{\log x} = li(x) - li(\alpha),$$

where x and α are both less, or both greater than 1. There will, of course, be no difficulty in understanding what is meant by

$$\int_0^x \frac{dx}{\log x}$$

taken along any path of integration which does not go through the point $x = 1$, provided that the particular value of log 0 with which we start is definitely assigned.

Gauss, in a letter to Encke (Werke, ii. p. 444), states that the number of primes which do not exceed x is approximately $\int \frac{dx}{\log x}$, the integral being given without any indication of the limits. In his tables of the frequency of primes, a comparison is made between the values of $F(\beta) - F(\alpha)$ and $\int_\alpha^\beta \frac{dx}{\log x}$ for successive intervals of 100,000 beginning with $\alpha = 1000{,}000$, and ending with $\alpha = 2900{,}000$; the comparison is also made for the intervals $10^6 \dots 2 . 10^6$ and $2 . 10^6 \dots 3 . 10^6$. It should be observed that Gauss's enumerations of the actual number of primes in the different intervals are not very accurate.

233. The mere fact that, so far as the enumeration of primes has been hitherto effected, the formula

$$F(x) = \int_2^x \frac{dx}{\log x}$$

is approximately correct, does not in any way prove that this is a proper asymptotic formula. It seems clear that Gauss was led to it simply by observation, and it does not appear that he ever accounted for it in any theoretical way. The only satisfactory attempt to determine a general analytical formula for $F(x)$ appears to be that contained in Riemann's celebrated memoir. This is confessedly incomplete, and the analysis which it contains is very peculiar and difficult: but because of its great importance, some account of it ought to be given. On the properties of the function $\Gamma(z)$ for a complex variable, which will have to be assumed in the course of the investigation, the reader may consult Prym, *Zur Theorie der Gammafunction* (Crelle, lxxxii. 165) and various papers by Bourguet and Mellin in vols. i. ii. iii. and viii. of the Acta Mathematica.

If x and s are complex quantities, we may define x^s to mean

$$e^{s \log x} = 1 + s \log x + \frac{s^2}{2} (\log x)^2 + \dots$$

and since $\log x$ is a many-valued function, x^s is many-valued also. If we write

$$\operatorname{Log} x = \int_1^x \frac{dx}{x}$$

where the integral is to be taken along a path from 1 to x which does not surround the origin, the general value of $\log x$ is

$\operatorname{Log} x + 2k\pi i$, where k is any integer, and the general value of x^s is therefore

$$x^s = e^{2ks\pi i} . e^{s \operatorname{Log} x}.$$

In what immediately follows we shall suppose that x^s stands for $e^{s \operatorname{Log} x}$, so that for instance when x is real and positive, and $s = \alpha + \beta i$,

$$\begin{aligned} x^s &= e^{(\alpha+\beta i) \operatorname{Log} x} \\ &= e^{\alpha \operatorname{Log} x} \{\cos (\beta \operatorname{Log} x) + i \sin (\beta \operatorname{Log} x)\} \end{aligned}$$

where $\operatorname{Log} x$ is the ordinary real logarithm of x.

This being so, then, whenever the real part of s is positive and greater than 1, we have

$$\Pi \frac{1}{1 - p^{-s}} = \Sigma n^{-s}$$

where the product on the left applies to all positive primes p, and the sum on the right to all positive integers n. This is easily seen by observing that, under the conditions stated, we may write

$$\begin{aligned} \frac{1}{1-2^{-s}} &= 1 + 2^{-s} + 2^{-2s} + \ldots \\ \frac{1}{1-3^{-s}} &= 1 + 3^{-s} + 3^{-2s} + \ldots \\ \ldots & \quad \ldots \quad \ldots \\ \frac{1}{1-p^{-s}} &= 1 + p^{-s} + p^{-2s} + \ldots \end{aligned}$$

where the series are absolutely convergent; and since n^{-s} can be expressed in one way only in the form

$$n^{-s} = p_1{}^{-\alpha s} . p_2{}^{-\beta s} p_3{}^{-\gamma s} \ldots$$

where p_1, p_2, p_3 etc. are different primes, and this term occurs once, and once only, in the expansion of $(1 + 2^{-s} + \ldots)(1 + 3^{-s} + \ldots) \ldots (1 + p^{-s} + \ldots) \ldots$ the proposition follows.

Now if n is a positive integer, and x a real variable, we may write

$$\int_0^\infty e^{-nx} x^{s-1} \, dx = n^{-s} \int_0^\infty e^{-y} y^{s-1} \, dy = n^{-s} \Gamma(s)$$

and hence

$$\Gamma(s) . \Sigma n^{-s} = \int_0^\infty (\Sigma e^{-nx}) x^{s-1} \, dx = \int_0^\infty \frac{x^{s-1} \, dx}{e^x - 1}.$$

We will now suppose the integral

$$\int \frac{x^{s-1}\,dx}{e^x - 1}$$

to be taken first along the axis of real quantities from $x = +\infty$ to $x = \epsilon$, where ϵ is a very small positive quantity, then in the positive direction along the circumference of a small circle of radius ϵ, with its centre at the origin, and finally along the axis of real quantities from $x = \epsilon$ to $x = +\infty$.

After going round the small circle, $\log x$ increases by $2\pi i$, and if we take x^s to mean (as above)

$$exp\left(s\int_1^x \frac{dx}{x}\right),$$

it is evident that, after describing the circle, $\dfrac{x^{s-1}}{e^x - 1}$ becomes $e^{2\pi is}\,.\,\dfrac{x^{s-1}}{e^x - 1}$. It is easily seen that if the real part of s exceeds 1, the integral round the circle vanishes ultimately when ϵ is infinitesimal: and therefore the whole integral is

$$(1 - e^{2\pi is})\int_\infty^0 \frac{x^{s-1}\,dx}{e^x - 1} = (e^{2\pi is} - 1)\int_0^\infty \frac{x^{s-1}\,dx}{e^x - 1}$$

$$= 2ie^{\pi is}\sin\pi s\int_0^\infty \frac{x^{s-1}\,dx}{e^x - 1}\,.$$

Comparing this with the previous result, we have

$$2\sin\pi s\,\Gamma(s)\,\Sigma n^{-s} = -ie^{-\pi is}\int_\infty^\infty \frac{x^{s-1}\,dx}{e^x - 1}$$

$$= i\int_\infty^\infty \frac{(e^{-\pi i}\,x)^{s-1}\,dx}{e^x - 1}$$

$$= i\int_\infty^\infty \frac{(-x)^{s-1}\,dx}{e^x - 1}$$

the integral on the right being taken along the path above defined. Observe that $(-x)^{s-1}$ is to be taken as $e^{-\pi i(s-1)}\,x^{s-1}$, where x^{s-1} is to have the same determination as in the equation

$$\Gamma(s) = \int_0^\infty e^{-x}\,x^{s-1}\,dx.$$

For convenience we may suppose $x^{s-1} = e^{(s-1)\,\mathrm{Log}\,x}$; but any other determination might be adopted, provided that the proper corresponding value of $\Gamma(s)$ be taken.

The path of the integration denoted by $\int_{\infty}^{\infty}$ may be modified in any way consistent with not including any of the zeroes of the function $(e^x - 1)$.

If, now, we define the function $\zeta(s)$ by means of the equation

$$2 \sin \pi s\, \Gamma(s)\, \zeta(s) = i \int_{\infty}^{\infty} \frac{(-x)^{s-1}\, dx}{e^x - 1}$$

$\zeta(s)$ is a one-valued function of s which is finite for all finite values of s except $s = 1$, and vanishes when s is a negative odd integer. Moreover when the real part of s exceeds 1, $\zeta(s) = \Sigma n^{-s}$.

When the real part of s is negative, the point $x = +\infty$ (a real quantity) is not a pole of the integral

$$\int \frac{(-x)^{s-1}\, dx}{e^x - 1}$$

and consequently the value of this integral, taken as above explained, is equal to the sum of the values of the same integral taken in the negative direction round infinitesimal circles each surrounding one of the poles $\pm 2\pi i$, $\pm 4\pi i$, etc.

The value of the integral taken round the pole $2n\pi i$ is

$$-2\pi i \,.\, \underset{x=2n\pi i}{\mathrm{Lt}} \frac{(x - 2n\pi i)(-x)^{s-1}}{e^x - 1} = -2\pi i\,(-2n\pi i)^{s-1}:$$

and in the same way that round the pole $-2n\pi i$ is

$$-2\pi i\,(2n\pi i)^{s-1}.$$

Substituting these values in the equation which defines $\zeta(s)$, we have

$$2 \sin \pi s\, \Gamma(s)\, \zeta(s) = (2\pi)^s \{i^{s-1} + (-i)^{s-1}\}\, \Sigma n^{s-1}$$
$$= (2\pi)^s \{i^{s-1} + (-i)^{s-1}\}\, \zeta(1-s)$$

or
$$2 \cos \frac{\pi s}{2}\, \Gamma(s)\, \zeta(s) = (2\pi)^s\, \zeta(1-s).$$

If in Legendre's formula

$$\Gamma(x)\, \Gamma\left(x + \frac{1}{n}\right) \ldots \Gamma\left(x + \frac{n-1}{n}\right) = (2\pi)^{\frac{n-1}{2}}\, n^{\frac{1}{2} - nx}\, \Gamma(nx)$$

we put $n = 2$, $x = \frac{s}{2}$, we obtain

$$\Gamma\left(\frac{s}{2}\right) \Gamma\left(\frac{1+s}{2}\right) = (2\pi)^{\frac{1}{2}} \,.\, 2^{\frac{1}{2}-s}\, \Gamma(s)$$
$$= 2^{1-s}\, \pi^{\frac{1}{2}}\, \Gamma(s).$$

Also $$\Gamma\left(\frac{1+s}{2}\right)\Gamma\left(\frac{1-s}{2}\right)=\frac{\pi}{\sin\frac{(1-s)\pi}{2}}=\frac{\pi}{\cos\frac{s\pi}{2}};$$

and therefore, eliminating $\Gamma\left(\frac{1+s}{2}\right)$,

$$2\Gamma(s)\Gamma\left(\frac{1-s}{2}\right)\cos\frac{s\pi}{2}=2^s\pi^{\frac{1}{2}}\Gamma\left(\frac{s}{2}\right).$$

Hence the relation connecting $\zeta(s)$ and $\zeta(1-s)$ may be written in the form

$$\Gamma\left(\frac{s}{2}\right)\zeta(s)=\pi^{s-\frac{1}{2}}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s)$$

or, which is the same thing,

$$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s)=\pi^{-\frac{1-s}{2}}\Gamma\left(\frac{1-s}{2}\right)\zeta(1-s).$$

This naturally suggests the introduction of the function $\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s)$ instead of $\zeta(s)$; this function is unaltered by the change of s into $1-s$.

Since $$n^{-s}\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)=\int_0^\infty e^{-n^2\pi x}x^{\frac{s}{2}-1}\,dx$$

it follows that $$\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)\zeta(s)=\int_0^\infty\psi(x)\,x^{\frac{s}{2}-1}\,dx,$$

where $$\psi(x)=\sum_1^\infty e^{-n^2\pi x}.$$

The function $\psi(x)$ is one of those which occur in the theory of elliptic functions; in fact, writing K'/K for x, and putting $e^{-\pi K'/K}=q$,

$$1+2\psi(x)=1+2q+2q^4+2q^9+\dots$$
$$=\sqrt{\frac{2K}{\pi}}.$$

Interchanging the moduli, so that x becomes $\frac{1}{x}$, we have

$$1+2\psi\left(\frac{1}{x}\right)=\sqrt{\frac{2K'}{\pi}}=x^{\frac{1}{2}}\{1+2\psi(x)\};$$

and hence $$\int_0^\infty\psi(x)\,x^{\frac{s}{2}-1}\,dx=\int_0^1\psi(x)\,x^{\frac{s}{2}-1}\,dx+\int_1^\infty\psi(x)\,x^{\frac{s}{2}-1}\,dx$$

$$=\int_0^1\left\{x^{-\frac{1}{2}}\psi\left(\frac{1}{x}\right)+\tfrac{1}{2}x^{-\frac{1}{2}}-\tfrac{1}{2}\right\}x^{\frac{s}{2}-1}\,dx+\int_1^\infty\psi(x)\,x^{\frac{s}{2}-1}\,dx$$

$$=\int_1^\infty\psi(x)\,\{x^{\frac{s}{2}-1}+x^{-\frac{s}{2}-\frac{1}{2}}\}\,dx+\frac{1}{s(s-1)}.$$

Now write
$$s = \tfrac{1}{2} + ti,$$
$$\frac{s(s-1)}{2}\,\pi^{-\frac{s}{2}}\,\Gamma\left(\frac{s}{2}\right)\zeta(s) = \xi(t);$$
then, on substitution, we find
$$\xi(t) = \tfrac{1}{2} - \tfrac{1}{2}(t^2 + \tfrac{1}{4})\int_1^\infty \psi(x)\left\{x^{-\frac{3}{4}+\frac{ti}{2}} + x^{-\frac{3}{4}-\frac{ti}{2}}\right\}dx$$
$$= \tfrac{1}{2} - (t^2 + \tfrac{1}{4})\int_1^\infty x^{-\frac{3}{4}}\psi(x)\cos(\tfrac{1}{2}t\log x)\,dx$$
where, of course, the determination of $\cos(\frac{1}{2}t\log x)$ must be in accordance with that of $\pi^{-\frac{s}{2}}\Gamma\left(\frac{s}{2}\right)$, in order that $\zeta(s)$ may be one-valued.

In order that the real part of s may be greater than 1, so that Σn^{-s} may converge, we must have
$$t = \alpha - \beta i$$
with
$$\beta > \tfrac{1}{2}.$$

If, in the expression for $\xi(t)$, we suppose the integration to be taken along the axis of real quantities, and $\log x$ to denote the real logarithm of x, we obtain an expression of the form
$$\xi(t) = A_0 + A_1 t^2 + A_2 t^4 + \ldots$$
where $A_0\, A_1\, A_2 \ldots$ are real coefficients. This particular value of $\xi(t)$ is always real when t is a pure imaginary, or, which is the same thing, whenever s is real. If s is a real quantity greater than 1, this value of $\xi(t)$ coincides with the real value of
$$\frac{s(s-1)}{2}\,\pi^{-\frac{s}{2}}\,\Gamma\left(\frac{s}{2}\right)\Sigma n^{-s}.$$

The coefficients A_i depend upon integrals of the type
$$\frac{2^{-r}}{(2r)!}\int_1^\infty x^{-\frac{3}{4}}\psi(x)\,.\,(\log x)^{2r}\,dx,$$
and it is easy to see that these diminish very rapidly as r increases, and that the expansion of $\xi(t)$ converges absolutely for all finite values of t.

Since, when the real part of s exceeds 1, the function of s with which $\xi(t)$ then coincides, never vanishes for finite values of s, it follows that the finite roots of the transcendental equation $\xi(t) = 0$ must all be of the form
$$\tau = \alpha \pm \beta i$$
with
$$\beta \not> \tfrac{1}{2}.$$

Now the number of roots of $\xi(t)=0$ contained within any simple contour is equal to

$$\frac{1}{2\pi i}\int d\log\xi(t)$$

taken in the positive direction round the contour. Riemann states without proof that the number of roots of $\xi(t)=0$ contained within the rectangle bounded by the lines $x=0$, $x=T$, $y=\pm\frac{1}{2}$, is found by this method to be approximately

$$\frac{T}{2\pi}\left(\log\frac{T}{2\pi}-1\right)$$

when T is large; the error being comparable with $\frac{1}{T}$. It follows from this that the frequency (or 'density') of the roots in the neighbourhood of the line $x=T$ is asymptotically

$$\frac{d}{dT}\left\{\frac{T}{2\pi}\left(\log\frac{T}{2\pi}-1\right)\right\}=\frac{1}{2\pi}\log\frac{T}{2\pi},$$

and hence we may write

$$\log\xi(t)=\Sigma\log\left(1-\frac{t^2}{\tau^2}\right)+\log\xi(0)$$

where the summation applies to all the roots τ of the equation $\xi(t)=0$. Riemann adds that, although he has not succeeded in proving it, it seems very probable that all the roots of $\xi(t)=0$ are real.

Let us now denote by $F(x)$ the number of primes which are less than x, when x itself is not a prime; when x is a prime let $F(x)$ stand for the number of primes less than x, increased by $\frac{1}{2}$, so that at every point where $F(x)$ changes abruptly

$$F(x)=\tfrac{1}{2}\{F(x-0)+F(x+0)\}.$$

Let s be a quantity of which the real part exceeds 1; then

$$\begin{aligned}\log\zeta(s)&=-\Sigma\log(1-p^{-s})\\&=\Sigma p^{-s}+\tfrac{1}{2}\Sigma p^{-2s}+\tfrac{1}{3}\Sigma p^{-3s}+\ldots.\end{aligned}$$

Now $$p^{-s}=s\int_p^\infty x^{-s-1}\,dx,\quad p^{-2s}=s\int_{p^2}^\infty x^{-s-1}\,dx,$$

and so on; and if these values are substituted in the expansion of $\log\zeta(s)$ we obtain an expression of the form

$$s\int_2^\infty f(x)\,x^{-s-1}\,dx.$$

where $f(x)$ is obtained by taking 1 for every prime which is less than x, $\frac{1}{2}$ for every square of a prime which is less than x, $\frac{1}{3}$ for every cube of a prime which is less than x, and so on; that is

$$f(x) = F(x) + \tfrac{1}{2}F(x^{\frac{1}{2}}) + \tfrac{1}{3}F(x^{\frac{1}{3}}) + \ldots,$$

because if $p^2 < x$, it follows that $p < x^{\frac{1}{2}}$, and the number of primes for which this condition is satisfied is $F(x^{\frac{1}{2}})$, and similarly for the other terms. There will of course be abrupt changes in $f(x)$ when x is a prime or a power of a prime, but since these critical values are separated by finite intervals, the expression $\int_2^\infty f(x)\, x^{-s-1}\, dx$ is perfectly definite.

When x is less than 2, $f(x) = 0$, so that we may write

$$\frac{\log \zeta(s)}{s} = \int_0^\infty f(x)\, x^{-s-1}\, dx$$

provided that $s = a + bi$, with $a > 1$.

Observing that $f(x)$ is real throughout the integration, we have

$$\frac{\log \zeta(s)}{s} = \int_0^\infty f(x)\, x^{-a} \{\cos(b \log x) - i \sin(b \log x)\}\, d \log x,$$

and from this, by Fourier's theorem, it follows that

$$2\pi x^{-a} f(x) = \int_{-\infty}^{+\infty} \frac{\log \zeta(s)}{s} \{\cos(b \log x) + i \sin(b \log x)\}\, db,$$

and therefore, multiplying both sides by ix^a,

$$2\pi i f(x) = \int_{a-i\infty}^{a+i\infty} \frac{\log \zeta(s)}{s}\, x^s\, ds,$$

the integration being taken along a straight line, so that the real part of s remains constant.

From the way in which $F(x)$ was defined it will be seen that this formula holds good for all real values of x, including those for which $f(x)$ changes abruptly.

Since $\frac{\log \zeta(s)}{s} x^s$ vanishes when $s = a \pm \infty i$, we find by partial integration that

$$2\pi i f(x) = -\frac{1}{\log x} \int_{a-\infty i}^{a+\infty i} \frac{d}{ds}\left(\frac{\log \zeta(s)}{s}\right) x^s\, ds$$

From the definition of $\xi(t)$

$$\zeta(s) = \frac{2}{s(s-1)} \frac{\pi^{\frac{s}{2}}}{\Gamma\left(\frac{s}{2}\right)} \xi(t)$$

$$= \frac{\pi^{\frac{s}{2}}}{(s-1)\Gamma\left(\frac{s}{2}+1\right)} \xi(t),$$

and therefore

$$\log \zeta(s) = \frac{s}{2}\log\pi - \log(s-1) - \log\Gamma\left(\frac{s}{2}+1\right) + \log\xi(t)$$

$$= \frac{s}{2}\log\pi - \log(s-1) - \log\Gamma\left(\frac{s}{2}+1\right)$$

$$+ \Sigma \log\left\{1 + \frac{(s-\frac{1}{2})^2}{\tau^2}\right\} + \log\xi(0).$$

Hence

$$\frac{d}{ds}\left(\frac{\log\zeta(s)}{s}\right) = -\frac{d}{ds}\left\{\frac{1}{s}\log\Gamma\left(\frac{s}{2}+1\right)\right\} - \frac{d}{ds}\left\{\frac{1}{s}\log(s-1)\right\}$$

$$+ \frac{d}{ds}\left[\frac{1}{s}\Sigma\log\left\{1+\frac{(s-\frac{1}{2})^2}{\tau^2}\right\}\right] - \frac{\log\xi(0)}{s^2}.$$

Now

$$-\log\Gamma\left(\frac{s}{2}+1\right) = \underset{m=\infty}{\mathrm{Lt}}\left(\sum_{n=1}^{n=m}\log\left(1+\frac{s}{2n}\right) - \frac{s}{2}\log m\right)$$

and therefore

$$-\frac{d}{ds}\left\{\frac{1}{s}\log\Gamma\left(\frac{s}{2}+1\right)\right\} = \sum_1^\infty \frac{d}{ds}\left\{\frac{1}{s}\log\left(1+\frac{s}{2n}\right)\right\}.$$

Also

$$\frac{d}{ds}\left[\frac{1}{s}\log\left\{1+\frac{(s-\frac{1}{2})^2}{\tau^2}\right\}\right] = \frac{d}{ds}\left[\frac{1}{s}\log\left(1-\frac{s}{\frac{1}{2}+\tau i}\right) + \frac{1}{s}\log\left(1-\frac{s}{\frac{1}{2}-\tau i}\right)\right]$$

$$- \frac{1}{s^2}\log\frac{\tau^2+\frac{1}{4}}{\tau^2}.$$

Consequently

$$\frac{d}{ds}\left\{\frac{1}{s}\log\zeta(s)\right\} = \sum_1^\infty \frac{d}{ds}\left\{\frac{1}{s}\log\left(1+\frac{s}{2n}\right)\right\}$$

$$+ \Sigma\frac{d}{ds}\left[\frac{1}{s}\log\left(1-\frac{s}{\frac{1}{2}+\tau i}\right) + \frac{1}{s}\log\left(1-\frac{s}{\frac{1}{2}-\tau i}\right)\right]$$

$$- \frac{d}{ds}\left\{\frac{1}{s}\log(s-1)\right\} - \frac{C}{s^2},$$

where $$C = \log \xi(0) + \Sigma \log\left(1 + \frac{1}{4\tau^2}\right).$$

The integral

$$\int_{a-\infty i}^{a+\infty i} \frac{1}{s^2} x^s ds = \int_{a-\infty i}^{a+\infty i} \frac{x^s \log x}{s} ds$$

$$= ix^a \log x \int_{-\infty}^{+\infty} \frac{\cos(b \log x) + i \sin(b \log x)}{a+ib} db$$

$$= 2ix^a \log x \int_0^\infty \frac{a \cos(b \log x)\, db}{a^2+b^2}$$

$$= 2ix^a \log x \,.\, \pi e^{-a \log x} = 2\pi i \log x$$

(as may also be seen by replacing the straight line of the original integration by a small circle round the pole $s = 0$).

All the other integrals in the expression for $2\pi i f(x) \log x$ may be reduced to the type

$$\int_{a-\infty i}^{a+\infty i} \frac{d}{ds}\left\{\frac{1}{s} \log\left(1 - \frac{s}{\beta}\right)\right\} x^s ds.$$

Call this $\phi(\beta)$; then

$$\phi'(\beta) = \int_{a-\infty i}^{a+\infty i} \frac{d}{ds}\left\{\frac{1}{\beta(\beta - s)}\right\} x^s ds$$

$$= -\frac{\log x}{\beta} \int_{a-\infty i}^{a+\infty i} \frac{x^s ds}{\beta - s},$$

on integrating by parts.

Now if the real part of β is less than the real part of s, so that the point β is on the left of the line along which the integral is taken, we may change the path of integration into a small circle described in the positive direction round the pole $s = \beta$. Hence the value of the integral is

$$\phi'(\beta) = \frac{2\pi i x^\beta \log x}{\beta}$$

$$= 2\pi i \log x \int_\infty^x x^{\beta-1} dx \text{ or } 2\pi i \log x \int_0^x x^{\beta-1} dx,$$

according as the real part of β is negative or positive.

Hence in the first case

$$\phi(\beta) = 2\pi i \log x \left\{\int_\infty^x \frac{x^{\beta-1}}{\log x} dx + A\right\},$$

and in the second

$$\phi(\beta) = 2\pi i \log x \left\{ \int_0^x \frac{x^{\beta-1}}{\log x}\, dx + B \right\},$$

where A and B are constants depending upon the way in which $\log\left(1 - \dfrac{s}{\beta}\right)$ is defined and on the paths along which the integrals are taken. In the second integral the path from 0 to x must not go through the critical point $x = 1$. We may, if we like, suppose that the integration from 0 to x is taken along the axis of real quantities from 0 to $1 - \epsilon$, then along a semicircle of radius ϵ from $(1 - \epsilon)$ to $(1 + \epsilon)$ and then along the axis of real quantities from $1 + \epsilon$ to x. Similarly we may suppose the integration from ∞ to x to be taken along the axis of real quantities.

The values of β are -2, -4, -6, etc., unity, and the different values of $\frac{1}{2} \pm \tau i$; and since a, the real part of s, is supposed greater than 1, we have finally

$$f(x) = \int_0^x \frac{dx}{\log x} - \sum_\tau \int_0^x \frac{x^{-\frac{1}{2}+\tau i} + x^{-\frac{1}{2}-\tau i}}{\log x}\, dx$$

$$+ \int_x^\infty (x^{-3} + x^{-5} + \dots)\frac{dx}{\log x} + C''$$

$$= \int_0^x \frac{dx}{\log x} - 2\sum_\tau \int_0^x \frac{x^{-\frac{1}{2}} \cos(\tau \log x)\, dx}{\log x} + \int_x^\infty \frac{dx}{x(x^2-1)\log x} + C',$$

C'' being a constant, the value of which will depend on the determination of $\log x$ in the integrals.

Observing that $\int_0^x \phi(x)\, dx$ only differs from $\int_2^x \phi(x)\, dx$ by a constant, and that $f(2) = \frac{1}{2}$, we may write, for $x > 2$,

$$f(x) = \int_2^x \frac{dx}{\log x} - 2\Sigma \int_2^x \frac{x^{-\frac{1}{2}} \cos(\tau \log x)\, dx}{\log x}$$

$$- \int_2^x \frac{dx}{x(x^2-1)\log x} + \tfrac{1}{2},$$

and take $\log x$ to mean throughout the real logarithm of x; the integrations, also, being taken along the axis of real quantities.

Neglecting terms which are comparatively very small when x is large,

$$f'(x) = \frac{1}{\log x} - 2\Sigma \frac{x^{-\frac{1}{2}} \cos(\tau \log x)}{\log x}.$$

It will be remembered that

$$f(x) = F(x) + \tfrac{1}{2}F(x^{\frac{1}{2}}) + \tfrac{1}{3}F(x^{\frac{1}{3}}) + \ldots,$$

and from this it may be inferred that

$$\begin{aligned} F(x) &= f(x) - \tfrac{1}{2}f(x^{\frac{1}{2}}) - \tfrac{1}{3}f(x^{\frac{1}{3}}) - \tfrac{1}{5}f(x^{\frac{1}{5}}) \\ &\qquad + \tfrac{1}{6}f(x^{\frac{1}{6}}) - \tfrac{1}{7}f(x^{\frac{1}{7}}) - \tfrac{1}{11}f(x^{\frac{1}{11}}) - \ldots \\ &= \Sigma\,(-1)^{\mu}\,\frac{1}{m}f\left(x^{\frac{1}{m}}\right), \end{aligned}$$

where m assumes all positive values not divisible by any square, and μ is the number of different prime factors of m.

To prove this, let n be any positive integer greater than 1, and let m, m' be any two conjugate factors of n so that $mm' = n$: then the coefficient of $F\left(x^{\frac{1}{n}}\right)$ in $\Sigma\,(-1)^{\mu}\,\frac{1}{m}f\left(x^{\frac{1}{m}}\right)$ is

$$\Sigma\,(-1)^{\mu}\,\frac{1}{m}\cdot\frac{1}{m'} = \frac{1}{n}\,\Sigma\,(-1)^{\mu},$$

where the sum is obtained by calculating μ for every divisor of n, 1 and n inclusive. But if n contains k prime factors, it is obvious that

$$\Sigma\,(-1)^{\mu} = 1 - k + \frac{k(k-1)}{2} - \frac{k(k-1)(k-2)}{3\,!} + \ldots = (1-1)^{k} = 0,$$

because there is one factor of n for which $\mu = 0$, there are k for which $\mu = 1$, $\frac{k(k-1)}{2}$ for which $\mu = 2$ and so on.

Thus all the functions $F\left(x^{\frac{1}{n}}\right)$ disappear except $F(x)$, which occurs once with a coefficient 1: and this proves the theorem.

Substituting the values of $f(x)$, $f(x^{\frac{1}{2}})$, etc. in the formula, we obtain an expression for $F(x)$.

Let $$B = \tfrac{1}{2} - \int_{2}^{\infty}\frac{dx}{x(x^{2}-1)\log x},$$

and let A denote the constant

$$\begin{aligned} A &= B(1 - \tfrac{1}{2} - \tfrac{1}{3} - \tfrac{1}{5} + \ldots) \\ &= B\Sigma\,(-1)^{\mu}\,\frac{1}{m}; \end{aligned}$$

then if we neglect the integrals $\int_2^x \frac{x^{-\frac{1}{2}} \cos(\tau \log x)\, dx}{\log x}$ we obtain the approximate value

$$F(x) = A + \Sigma (-1)^{\mu} \frac{1}{m} L\left(x^{\frac{1}{m}}\right),$$

where
$$L(x) = \int_2^x \frac{dx}{\log x}.$$

Since A is a finite quantity, it may be omitted without sensibly affecting the formula when x is very large.

We conclude from this result that Gauss's approximate value is ultimately too large; and this is confirmed by the comparisons given by Gauss for the second and third millions.

AUTHORITIES.

Legendre: *D'une loi très-remarquable observée dans l'énumération des nombres premiers* (Essai sur la théorie des nombres, 2nd ed. (1808) Part IV. § VIII.).

Gauss: *Tafel der Frequenz der Primzahlen* (Werke ii. p. 435); followed by a letter to Encke (ibid. p. 444).

Tchébicheff: *Sur la fonction qui détermine la totalité des nombres premiers inférieurs à une limite donnée* (Mém. de l'Acad. de St Pétersbourg (Savans Etrangers) vol. vi. (1851) p. 141; reprinted in Liouv. xvii. (1852) p. 341).

Mémoire sur les nombres premiers (Mém. de l'Acad. de St Pétersbourg (*ut supra*) vol. vii. (1854) p. 15; or Liouv. xvii. (1852) p. 366).

Riemann: *Ueber die Anzahl der Primzahlen unter einer gegebenen Grösse* (Monatsber. der Akad. d. Wiss. zu Berlin for 1859; or Werke, p. 136).

Meissel: *Ueber die Bestimmung der Primzahlmenge innerhalb gegebener Grenzen* (Math. Ann. ii. (1870) p. 636).

Berechnung der Menge von Primzahlen, welche innerhalb der ersten hundert Millionen natürlichen Zahlen vorkommen (Math. Ann. iii. (1871) p. 523).

Rogel: *Zur Bestimmung der Anzahl Primzahlen unter gegebenen Grenzen* (Math. Ann. xxxvi. (1890) p. 304).

Sylvester: *On Arithmetical Series* (Messenger of Math. vol. xxi. (1891); see also a previous paper by the same author, Amer. Journ. iv. p. 241).

Poincaré: *Extension aux nombres premiers complexes des théorèmes de M. Tchébicheff* (Liouv. (4) viii. (1892) p. 25).

EXAMPLES.

1. Prove that if, to the base 10,

$$\log\frac{1025}{1024}=a,\quad \log\frac{1024^2}{1023\,.\,1025}=b,\quad \log\frac{81^2}{80\,.\,82}=c,$$

$$\log\frac{125^2}{124\,.\,126}=d,\quad \log\frac{99^2}{98\,.\,100}=e,$$

then $$196\log 2 = 59+5a+8b-3c-8d+4e\,;$$

and find log 3 and log 41 in terms of the same quantities. (See Gauss, Werke ii. p. 501.)

2. Verify that $2^{4\mu+2}+1=(2^{2\mu+1}+2^{\mu+1}+1)(2^{2\mu+1}-2^{\mu+1}+1)$, and hence factorise $2^{58}+1$.

(This application of a familiar algebraical identity appears to be due to Aurifeuille: see Lucas, *Théorie des Nombres*, i. p. 326.)

3. From the facts that $10^m\equiv 1 \pmod 9$ and $10^m\equiv(-1)^m \pmod{11}$ deduce the ordinary criteria for the divisibility of any number by 9 or by 11.

Prove that a number expressed in any scale of notation is divisible by a given number m if a certain linear combination of its digits is divisible by m; and shew how the simplest combination in question may be discovered.

For example, prove that a number $a_n a_{n-1}\dots a_2 a_1$ expressed in the scale of 7 is divisible by 19 if

$$(a_1+a_4+a_7+\dots)+7(a_2+a_5+a_8+\dots)-8(a_3+a_6+a_9+\dots)$$
$$\equiv 0 \pmod{19}.$$

4. If p is an odd prime (except 5), and $a<p$, the fraction a/p may be expressed as a pure circulating decimal, and the number of figures in the period is equal to the exponent to which 10 appertains, mod p.

Calling this exponent f, the expansions of

$$\frac{1}{p},\ \frac{2}{p},\dots\frac{p-1}{p}$$

will give rise to $(p-1)/f$ groups of periods, the periods of each group being derived from each other by cyclical permutations of the digits: hence if one period of each group is known, and also the index of 10 to any primitive root of p, the index of any number may be determined. (*D. A.* Arts. 312—318.)

5. If $4n+3$ and $8n+7$ are both primes, then $2^{4n+3}-1$ is divisible by $8n+7$. (Euler.)

The numbers 2^p-1, where p is prime, are known as Mersenne's numbers. According to Mersenne (*Cogitata Physico-Mathematica*, (Paris, 1644) præfatio generalis, Art. 19) the only values of p, not exceeding 257, for which 2^p-1 is prime, are 1, 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257. Seelhoff has proved that $2^{61}-1$ is prime, but this is the only exception to Mersenne's statement yet discovered. See W. W. Rouse Ball *On Mersenne's Numbers* (Mess. of Math. xxi. (1891) p. 34) and Lucas, *Théorie des Nombres*, i. p. 374.

6. Prove that if 2^p-1 is a prime, then $2^{p-1}(2^p-1)$ is equal to the sum of its aliquot parts. (Euclid ix. 36.)

A number which is equal to the sum of its aliquot parts is called a *perfect number*. No method of finding perfect numbers, except Euclid's, has been discovered: it is not even known whether any odd perfect numbers exist. Euclid's formula includes all even perfect numbers: of these the first six are

6, 28, 496, 8128, 33550336, 8589869056,

and three others have been calculated (Rouse Ball and Lucas, as above).

7. A pack of 52 cards is shuffled in the following way. The top card is removed, and the card originally second is placed above it; then the card originally third is placed below the two cards already removed, and so on; the card which is at the top of the unshuffled part of the pack at any stage of the process being placed at the bottom or top of the other packet according as its place in the whole pack was odd or even originally. Prove that when this process has been repeated 12 times the cards come back to their original places.

In general, for a pack of $2n$ cards, the original order is first restored after m shuffles, where m is the least number for which $2^m \equiv \pm 1 \pmod{4n+1}$.

(On the history of this problem, known as 'Monge's shuffle,' see Bourget, Liouv. (3) viii. (1882) p. 413.)

8. Deduce from the theorem $\Sigma\phi(d)=n$ (Art. 8), that

$$\phi(m)=\begin{vmatrix} 1 & 0 & 0 & 0 & 0 & \ldots\ldots & 1 \\ 1 & 1 & 0 & 0 & 0 & \ldots\ldots & 2 \\ 1 & 0 & 1 & 0 & 0 & \ldots\ldots & 3 \\ 1 & 1 & 0 & 1 & 0 & \ldots\ldots & 4 \\ 1 & 0 & 0 & 0 & 1 & \ldots\ldots & 5 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots\ldots & \ldots \end{vmatrix},$$

where there are m rows and columns, the last column consisting of the natural numbers 1, 2, 3 ... m, and the elements of the rth column ($r < m$) being all zeroes with the exception of those elements whose places, reckoned from the top, are multiples of r, in which case the corresponding element is 1. (Hammond.)

9. If a, n are any integers, and $a^x \equiv 1 \pmod{n}$ for $x = n - 1$, but not when x is an aliquot part of $(n - 1)$, the integer n is a prime. (Lucas, *Théorie des Nombres*, i. p. 441.)

10. If m is any number, the product of all the integers prime to m, which remain prime to m when increased by 1, is congruent to 1 (mod m). For instance, if $m = 15$, the numbers are 1, 7, 13 and $1 . 7 . 13 \equiv 1 \pmod{15}$.

(Schemmel, Crelle lxx. (1869) p. 191.)

11. Every divisor of $x^{2^m} + y^{2^m}$ is of the form $2^{m+1} n + 1$.

(Euler, *Comm. Arith.* i. p. 55.)

12. The sum of the rth powers of the $\phi(m)$ numbers less than m and prime to it is

$$\frac{m^{r+1}}{r+1} \Pi \left(1 - \frac{1}{p}\right) + \frac{rB_1}{2\,!} m^{r-1} \Pi (1 - p) \\ - \frac{r(r-1)(r-2)B_3}{4\,!} m^{r-3} \Pi (1 - p^3) + \ldots$$

where the products refer to the different prime factors of m; $B_1 = \frac{1}{6}$, $B_3 = \frac{1}{30}$, etc. are the numbers of Bernoulli; and the series on the right-hand is to be continued so long as the terms involve positive powers of m (exclusive of m^0).

Verify the theorem for $m = 10$, $r = 7$.

13. If q and $p = 2^{m+2} q + 1$, where $m > 0$, are both odd primes, then 3 is a primitive root of p, provided that $2^{m+2} q > 9^{2m}$.

(Tchébicheff.)

14. If $p = 4n + 3$ is a prime number,

$$(2n + 1)\,! + (-1)^\mu \equiv 0 \pmod{p},$$

where μ is the number of quadratic non-residues of p which are less than $\frac{1}{2}p$.

(Jacobi, Crelle ix. p. 189: the problem is Dirichlet's.)

15. Verify the following congruences:

$$\begin{array}{lll}
2\,!+1\equiv 1\,.\,3 \quad (3^2), & 12\,!+1\equiv 0 \quad (13^2), & 28\,!+1\equiv 18\,.\,29\,(29^2),\\
4\,!+1\equiv 0 \quad (5^2), & 16\,!+1\equiv 5\,.\,17\,(17^2), & 30\,!+1\equiv 19\,.\,31\,(31^2),\\
6\,!+1\equiv 5\,.\,7 \quad (7^2), & 18\,!+1\equiv 2\,.\,19\,(19^2), & 40\,!+1\equiv 16\,.\,41\,(41^2).\\
10\,!+1\equiv 1\,.\,11\,(11^2), & 22\,!+1\equiv 8\,.\,23\,(23^2), &
\end{array}$$

Can any rule be discovered for finding primes p such that $(p-1)\,!+1\equiv 0 \pmod{p^2}$?

16. If $2n+1$ is an odd prime p,

$$(2n)\,!\equiv(-1)^n\,2^{4n}\,(n\,!)^2 \pmod{p^2}.$$

17. Can any rule be assigned for deciding *a priori* whether the diophantine equation $x^2-Dy^2=\pm 4$ admits of integral solutions in which x, y are both odd?

(Cf. Art. 153 and Cayley, Crelle liii. p. 369.)

18. If m and n assume all positive integral values, the expression

$$m+\frac{(m+n-1)(m+n-2)}{2}$$

assumes all positive integral values without exception and each value only once. (Cantor.)

19. The rth series of polygonal numbers being defined by the formula $\frac{1}{2}\{rn^2-(r-2)\,n\}$, prove that the series will contain an infinite number of squares, unless r is the double of a square number. (Euler, *Comm. Arith.* i. p. 9.)

20. If $E(x)$ denote the integral part of x, then (i) m and n being any two positive integers such that n is not a factor of m,

$$E\left(\frac{m}{n}\right)=\frac{m}{n}-\frac{1}{2}+\frac{1}{2n}\sum_{k=1}^{k=n-1}\sin\frac{2km\pi}{n}\cot\frac{k\pi}{n}\,;$$

(ii) m and n being any two odd positive integers prime to each other,

$$\sum_{k=1}^{k=\frac{1}{2}(n-1)}E\left(\frac{km}{n}\right)=\frac{n^2-1}{8}\,\frac{m}{n}-\frac{n-1}{4}-\frac{1}{2n}\sum_{k=1}^{k=\frac{1}{2}(n-1)}\tan\frac{km\pi}{n}\cot\frac{2k\pi}{n}\,;$$

(iii) if m and n are prime to each other, and both $\equiv 1 \pmod{\mu}$,

$$\sum_{h=1}^{h=(n-1)/\mu}E\left(\frac{hm}{n}\right)+\sum_{k=1}^{k=(m-1)/\mu}E\left(\frac{kn}{m}\right)=\frac{(m-1)(n-1)}{\mu^2}.$$

(Eisenstein, Crelle xxvii. p. 281.)

21. If p is an odd prime, and a an odd number prime to p, prove that $(a|p)=(-1)^T$, where

$$T=\frac{1}{2p}\left\{\frac{(a-2)p^2+2p-a}{4}-\sum_{k=1}^{k=\frac{1}{2}(p-1)}\tan\frac{ka\pi}{p}\cot\frac{2k\pi}{p}\right\}.$$

(Eisenstein *l. c.*)

22. Let $\theta(k)$ denote the excess of the number of divisors of k which are of the form $4n+1$ above the number of those which are of the form $4n+3$; then

$$\Sigma\theta(k)=E(m)-E\left(\frac{m}{3}\right)+E\left(\frac{m}{5}\right)-E\left(\frac{m}{7}\right)+\ldots,$$

the summation on the left extending from $k=1$ to $k=E(m)$.

Deduce from this that the number of points whose coordinates are integers (exclusive of the origin) contained within the circle $x^2+y^2=m$ is four times the number contained within the area bounded by the line $x=0$ and the hyperbolas

$$y(4x+1)=m, \quad y(4x+3)=m.$$

(Eisenstein, Crelle xxvii. p. 248 and Gauss, Werke ii. p. 292.)

23. Prove that when y assumes all positive integral values from 1 to $E\left(\frac{m}{5}\right)$, the number of the quantities $\frac{m}{4y}$ of which the fractional part is less than $\frac{3}{4}$ but not less than $\frac{1}{4}$ is

$$E\left(\frac{m}{5}\right)-E\left(\frac{m}{7}\right)+E\left(\frac{m}{9}\right)-E\left(\frac{m}{11}\right)+\ldots.$$

Generalise this proposition, and shew its connexion with last example.

24. Kronecker has stated the following proposition:—

Let $p=4n+3$ be a prime, and let (a_1, b_1, c_1), (a_2, b_2, c_2), etc. be the properly primitive reduced forms of all those negative determinants $-\Delta$ for which p is representable by the principal form $x^2+\Delta y^2$, with y uneven; then the roots of the congruences

$$a_ix^2+2b_ix+c_i\equiv 0 \pmod p$$

will all be real, and will form a complete system of residues to modulus p; double roots being reckoned once only. Verify this for $p=7, 11, 19$, etc. (Berlin Monatsber. 1862, p. 304.)

25. Prove that the sign of the symbol $(m|n)$, where m, n are both odd, is the same as that of

$$\Pi\left(\frac{h}{n}-\frac{k}{m}\right)\left(\frac{h}{n}+\frac{k}{m}-\frac{1}{2}\right) \qquad \begin{bmatrix} h=1,\,2,\,3\,\ldots\,\tfrac{1}{2}(n-1) \\ k=1,\,2,\,3\,\ldots\,\tfrac{1}{2}(m-1) \end{bmatrix},$$

and deduce the law of reciprocity. (Kronecker.)

26. If G is a large positive integer, we may write asymptotically

$$\sum_{1}^{G}\phi(m)=\frac{3}{\pi^2}G^2+\Delta,$$

where $$\Delta<(\tfrac{1}{2}\log G+\tfrac{1}{2}C+\tfrac{5}{8})\,G+1,$$

C being Euler's constant. (Mertens, Crelle lxxvii. p. 289.)

27. Representing by $h(\Delta)$ the number of positive properly primitive classes of determinant $-\Delta$, then, when G is large, we have asymptotically

$$\sum_{1}^{G}h(\Delta)=\frac{4\pi G^{\frac{3}{2}}}{21S_3},$$

where $$S_3=1+\frac{1}{2^3}+\frac{1}{3^3}+\frac{1}{4^3}+\ldots.$$

(Mertens *l. c.*; and Gauss, *D. A.* Art. 302, Werke ii. p. 284.)

INDEX.

[The numbers refer to the pages.]

[The numbers refer to the pages.]

[*The numbers refer to the pages.*]

Cambridge:
PRINTED BY C. J. CLAY, M.A. AND SONS,
AT THE UNIVERSITY PRESS.